Отчёт об исследовании утечек информации ограниченного доступа в 2021 году

Оглавление

Только факты

- ✓ Доля утечек с применением средств автоматизации выросла с 85,9% в 2018 г. до 95,5% в 2021 г.
- ✓ В 2021 году более чем на 28% по сравнению с 2020 годом сократилось количество публикаций об утечках информации ограниченного доступа.
- ✓ Количество скомпрометированных записей персональных и платежных данных в рамках таких публично известных утечек в мире также снизилось более чем на 28%.
- ✓ Доля утечек, вызванных внешними нарушителями, за четыре года выросла с 35,6% до 63,2%.
- ✓ 82% утечек в мире спровоцированы умышленными действиями.
- ✓ Доля умышленных нарушений среди утечек внутреннего характера (по вине персонала) в последние два года составляет более 51%.
- ✓ Основным каналом утечки информации в 2021 году осталась Сеть, ее доля превысила 75%. Доли других каналов сократились.

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 группы компаний InfoWatch представляет исследование случаев утечек информации ограниченного доступа, зарегистрированных в 2021 году. В отчетах за 2020 год мы отмечали, что пандемия оказала сильнейшее влияние на многие сферы жизни, а значит, подействовала и на формирование картины утечек. Можно сказать, что в 2021 г. новая реальность продолжила играть ключевую роль в жизни людей во всем мире. Ускоренными темпами развивались дистанционные каналы обслуживания, искусственный интеллект, ИТ-сервисы. Удаленная (или как минимум комбинированная) работа стала нормой для сотен миллионов людей по всему миру. На этом фоне еще быстрее меняется ландшафт угроз информационной безопасности. Все это отражается и на структуре утечек информации ограниченного доступа. Обо всех ключевых изменениях мы расскажем в этом отчете.

Результаты исследования

В ходе подготовки данных для исследования мы не только тщательно проанализировали произошедшие в 2021 году утечки, но и внесли коррективы в данные за 2018-2020 годы, в т.ч. по результатам вновь вскрывшихся обстоятельств удалили некоторые из них, одновременно добавили новую информацию, ставшую известной из различных источников.

В рассматриваемом временном периоде аномальным как по количеству утечек, так и по количеству утекших данных отмечен 2019 год. В следующем, «пандемийном» 2020 году оба показателя сократились. По итогам 2021 г. Экспертно-аналитический центр InfoWatch на основе изучения открытых источников зарегистрировал 1729 случаев утечки информации ограниченного доступа из коммерческих компаний, государственных организаций и органов власти во всем мире. Это на 28,1% меньше, чем за аналогичный период 2020 г. – в результате корректировки и добавления данных за тот период аналитики ЭАЦ насчитали 2406 утечек.

Всего за 2021 г. «утекло» 8,42 млрд записей персональных (ПДн) и платежных данных. Это на 28,8% меньше, чем 2020 г., когда, по уточненным данным, количество утекших записей составило более 11,82 млрд. Таким образом, снижение количества случаев утечек коррелирует со снижением количества скомпрометированных записей.

В то же время мы видим, что количество «утекших» записей как 2021, так и 2020 годов превышает показатели 2018 года.

> *TechCrunch: В даркнете выставили на продажу персональные данные почти 100 млн подписчиков платежного приложения, разработанного индийским стартапом MobiKwik. По словам неизвестных продавцов, всего у них есть порядка 8,2 ТБ данных: номера телефонов, адреса электронной почты, зашифрованные пароли, журналы транзакций и части номеров платежных карт. Стоимость доступа к базе данных на подпольном форуме оценили примерно $70 тыс.*
>
> *The Wall Street Journal: Китайская компания Alibaba Group потерпела крупнейшую утечку конфиденциальной информации в своей истории – по вине одного из программистов оказались скомпрометированы персональные данные более 1 миллиарда клиентов магазина TaoBao. Согласно приговору китайского суда, разработчик ПО в течение восьми месяцев копировал конфиденциальную информацию с популярной платформы интернет-торговли Taobao. Используя специально созданную программу для сканирования сетевых ресурсов, недобросовестный сотрудник смог скопировать персональные данные более 1,1 млрд человек, прежде чем в Alibaba заметили подозрительную активность в своей сети.*

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

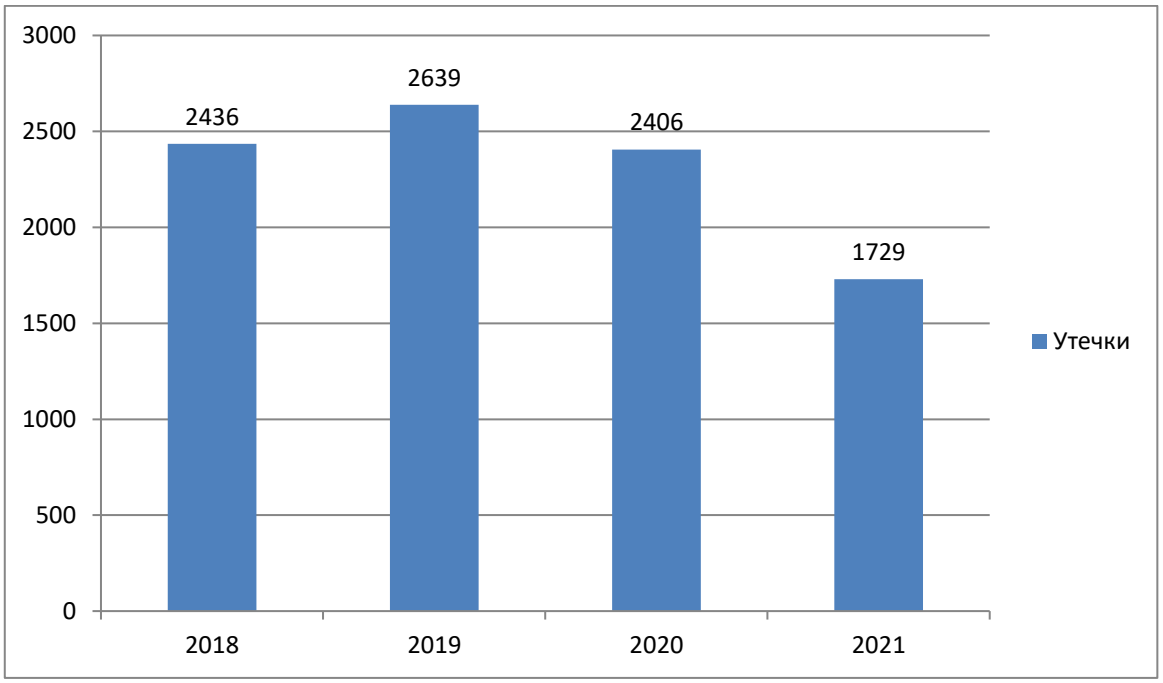


Рисунок 1. Число зарегистрированных утечек: Мир, 2018-2021 гг.

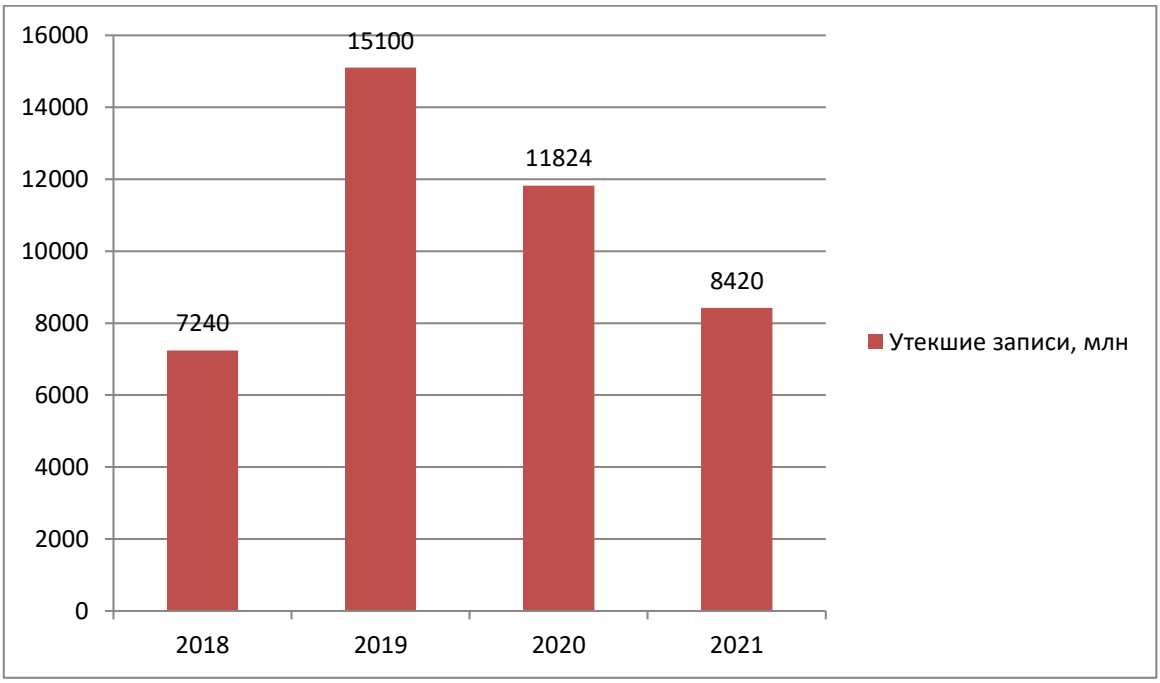


Рисунок 2. Количество утекших записей: Мир, 2018-2021 гг.

Снижение количества известных (опубликованных в СМИ и других открытых источниках) случаев утечек в 2020-2021 г. может объясняться несколькими факторами. Во-первых, в пандемию во многих компаниях объективно ослаб контроль за информационными ресурсами, в результате подводная часть «айсберга утечек» могла стать еще более значительной.

Во-вторых, в ряде компаний, прежде всего, крупных, начали приносить плоды организационно-технические мероприятия по защите информационной инфраструктуры, в том числе внедрение DLP-систем, а также ряд действий в начале пандемии.

В-третьих, в «допандемийные» годы хакеры успели наворовать столько персональных и платежных данных, что Дарквебу потребовалось немало времени на «переваривание» таких объемов информации – подпольному рынку хватало источников для продажи и перепродажи как похищенных баз целиком, так и отдельных фрагментов. Тем более, что в ряде стран среди мошеннических схем на первое место вышли схемы, связанные с соцпомощью, дотациями и другими мерами поддержки пострадавших от пандемии. Для их получения достаточно было ПДн, включающих в себя ФИО, адрес и номер соцстрахования, которые редко меняются, то есть базы 2019 года сохраняли свою актуальность.

Также дельцы черного рынка активно занимались обогащением ранее сформированных баз, формируя некую «добавленную стоимость» для своего товара. Или просто немного дополняя и переименовывая сборники данных.

В-четвертых, в продаже появились базы, сформированные путем сканирования открытых источников, например, соцсетей. Их мы не относим к утечкам.

В-пятых, развитие вредоносного ПО привело к широкому распространению вирусов-вымогателей, операторы которых не всегда стремятся похитить данные – хакерам зачастую достаточно заблокировать доступ к ним или зашифровать их, а потом требовать выкуп.

По сути, если при краже данных внешними нарушителями действует схема «взлом – копирование данных – продажа данных – деньги», то в случае с шифрованием данных пользователя она выглядит так: «взлом – шифрование данных – деньги», исключая зачастую длительный и неопределенный по времени этап продажи (если, конечно, это не была заказная акция).

Остановка бизнес-процессов в результате шифрования данных и последующей блокировки информационных систем, цифровых сервисов – это крайне болезненная ситуация для большинства компаний, причем не всегда помогает наличие резервных копий, так как необходимо время на восстановление и тестирование. Поэтому в подобной ситуации бизнес зачастую идёт на диалог с киберпреступниками и вносит требуемый выкуп.

То есть «конверсию» атак хакеры чаще стали рассматривать под другим углом – «прямой монетизации» данных в деньги (выкуп за расшифровку), исключив процесс поиска покупателей данных и непосредственной продажи, снизив тем самым количество объявлений в Дарквебе и, как следствие, повлияв на снижение публикаций об утечках в СМИ.

Интересные изменения произошли в структуре утечек с точки зрения вектора воздействия на информационные ресурсы (внешний/внутренний). Доля утечек по вине внешних нарушителей в 2021 г. по сравнению с 2020 годом выросла с 52,9% до 63,2%. Соответственно, в результате умышленных и случайных действий внутренних нарушителей произошло 36,8% утечек в 2021 г. и 47,1% в 2020 г. Вероятно, сыграло свою роль распространение удаленной работы, когда контроль за сотрудниками оказался сильно затруднен. В такой ситуации недобросовестные работники могли незаметно похищать информацию, кроме того, в тень мог уйти большой пласт случайных нарушений.

В целом, с 2018 г. наблюдается неуклонный рост доли утечек в результате действий внешних нарушителей. Это может быть связано со становлением широкого спектра хакерских группировок, повышением доступности вредоносного ПО (в том числе по мере развитие модели RaaS – «вредоносное ПО как услуга»). Вместе с тем, в ряде случаев возможно полагать, что утечки были совершены при участии сотрудников, вступивших в сговор с хакерами, или вследствие ошибок сотрудников, которые привели к раскрытию аутентификационной информации, которой воспользовались внешние нарушители. Но в других случаях, когда утечку удалось предотвратить или своевременно выявить, минимизировав ущерб, многие компании убедились в эффективности средств защиты, направленных на противодействие внутренним нарушениям. Речь идет о DLP-системах, решениях для контроля доступа, поведенческой аналитики и т.д.

> *Hindustan Times: Компания Jubilant FoodWorks, владеющая франшизой Domino's Pizza в Индии, признала факт утечки, в результате которой хакеры украли персональные данные порядка 180 млн клиентов. Скомпрометированные данные включают имена, адреса электронной почты, номера мобильных телефонов, GPS-координаты и другую информацию.*

Рост доли утечек в результате внешнего воздействия показан на Рисунке 3.

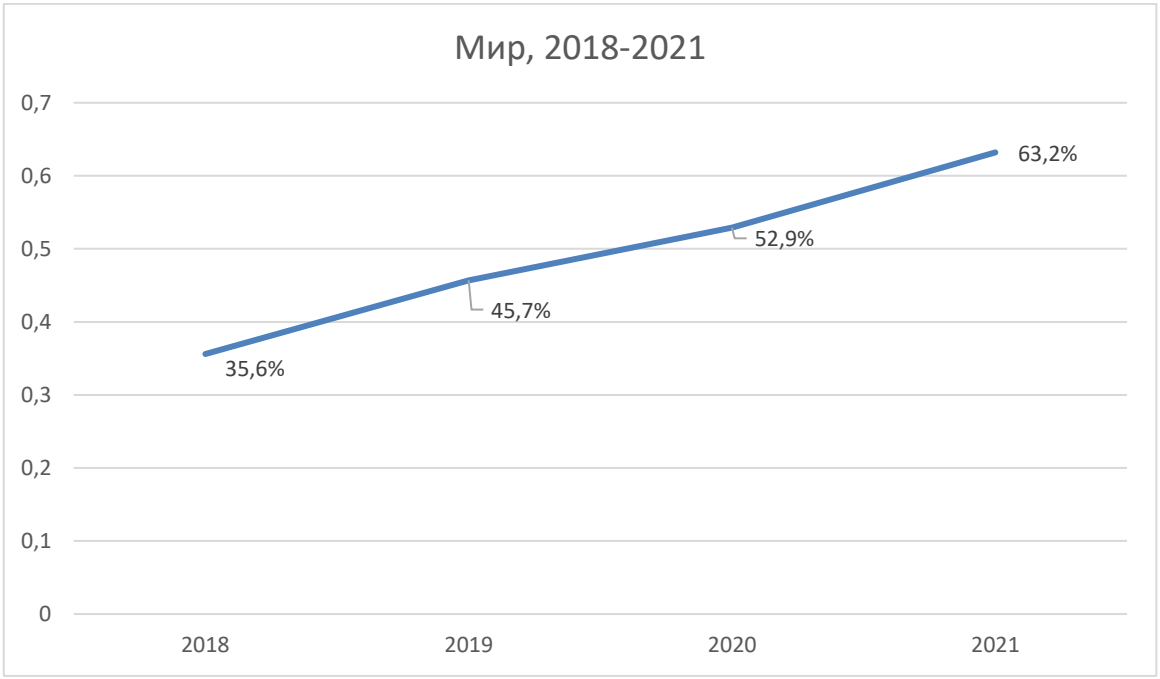


Рисунок 3. Динамика доли утечек вследствие внешнего воздействия: Мир 2018-2021гг.

Таким образом, если в 2018 г. на долю внутренних нарушителей пришлось примерно 2/3 случаев, то по итогам 2021 г. картина получилась практически зеркальной – почти в 2/3 всех внесенных опубликованных (ставших известными) утечек информации ограниченного доступа в качестве виновников указаны внешние нарушители.

Заявленные виновными не обязательно могут быть ответственны за утечки, так как в странах, где существует ответственность за сокрытие фактов утечек (прежде всего в США и в государствах ЕС; например, согласно требованиям GDPR, компания должна уведомить регулирующие органы об утечке в течение 72 часов), многим компаниям выгодно винить во всём хакеров, скрывая пробелы в организации безопасной удалённой работы и защищая свой имидж. Тем более, что перепроверить результаты их заявлений (отчётов) практически невозможно.

Латентность инцидентов (в большей степени нарушений внутреннего характера, в меньшей – внешних нарушений), вполне вероятно, стала следствием того, что компаниям теперь намного сложнее контролировать и без того сильно размытый информационный периметр. В связи с массовым переводом сотрудников на удаленную работу возникло множество новых уязвимых точек входа в корпоративные сети для злоумышленников, средств для защиты и контроля которых у многих компаний поначалу просто не было. В результате еще больше утечек могли остаться незамеченными владельцами (операторами) или оказались намеренно скрытыми. Соответственно, в таких случаях отсутствуют официальные публикации, извещения госорганов и данные о пострадавших гражданах (сотрудниках). Кроме того, компании из ряда стран, прежде всего, западных, стали более тщательно проводить расследования и подавать данные об утечках позже обычного, в результате чего

существенная часть нарушений, случившихся в 2021 году, скорее всего попадут в отчетность за 2022 год. В первом квартале 2022 г. на форумах в Даркнебе появилось довольно много данных, украденных в 2021 г. и даже раньше.

В пандемию темпы цифровизации во многих сферах резко ускорились, на первый план вышли дистанционные каналы обслуживания. В этой связи у каждой единицы информации о клиенте появилась вполне осязаемая ценность, персональные данные и другая конфиденциальная информация стали очень ликвидным товаром в Даркнебе. ПДн по-прежнему востребованы на черном рынке, даже несмотря на то, что, как мы отметили выше, хакеры не всегда ставят цель похитить их – для крупного заработка совсем не обязательно скачивать данные, достаточно просто заблокировать хранилища или зашифровать информационные активы.

В случае кражи информации внутренними нарушителями выявить утечку стало намного сложнее, если компания не внедрила системы контроля. В основном это связано с тем, что широкие группы сотрудников по-прежнему остаются на дистанционной работе. **Вероятно, латентность внутренних инцидентов как в мире, так и в России росла опережающими темпами в 2020-2021 гг.**

Доля умышленных случаев среди всех зарегистрированных утечек в глобальном масштабе тоже неуклонно растет. По итогам 2021 г. она достигла 82% (Рисунок 4).

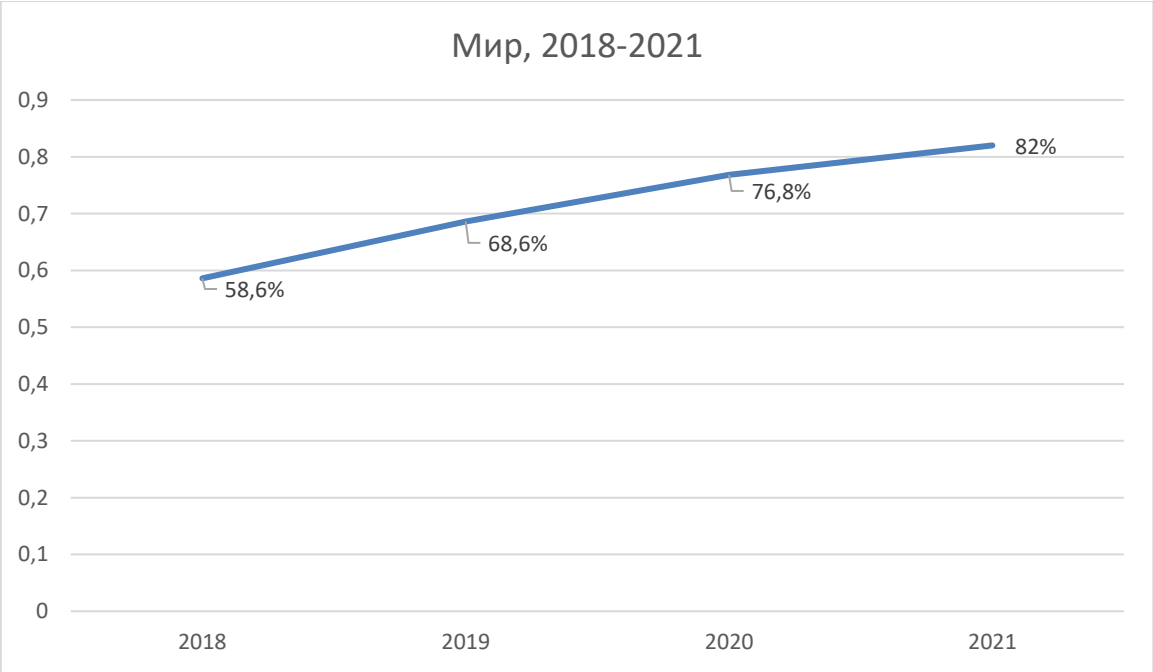


Рисунок 4. Динамика доли умышленных нарушений: Мир, 2018-2021 гг.

На Рисунке 5 представлены доли умышленных утечек по вине внутренних утечек.

Если посмотреть, каково соотношение утечек по вине внутренних и внешних нарушителей, то можно заметить, что некоторая часть компаний пытается скрыть информацию о внутренних нарушителях, иначе рост «внутренних» утечек коррелировал бы с графиком на рисунке 4.

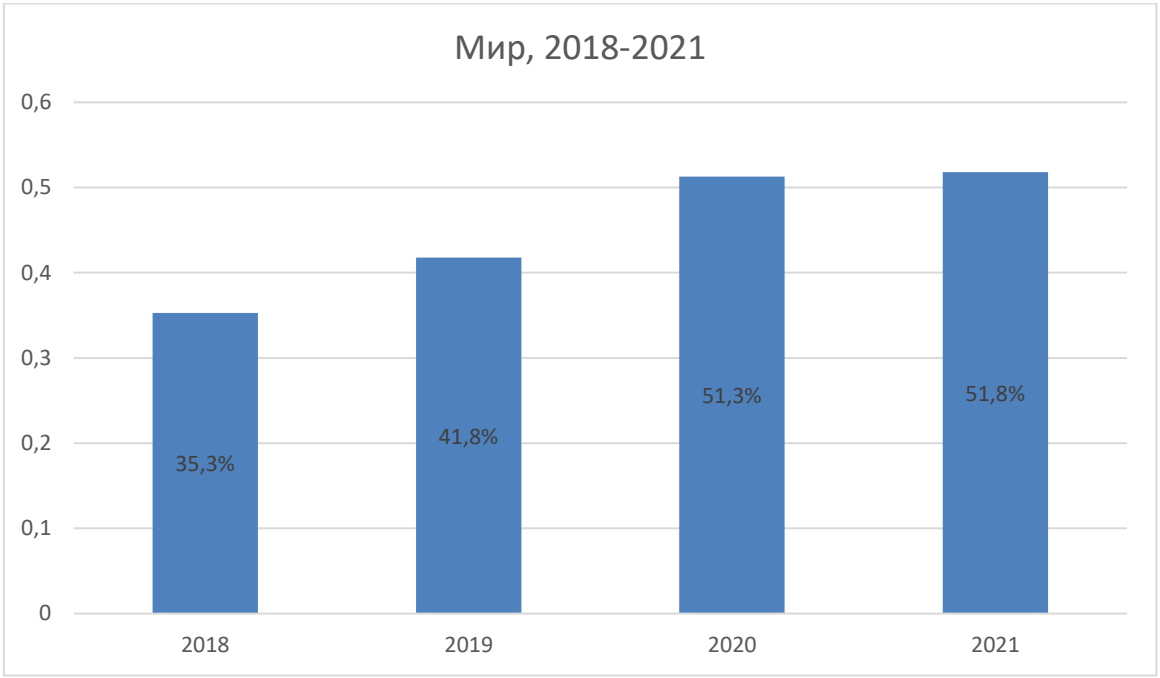


Рисунок 5. Динамика доли умышленных нарушений внутреннего характера: Мир, 2018-2021 гг.

Очевидно, что в условиях роста ликвидности конфиденциальной информации, особенно, персональных данных как основного артефакта цифровой эпохи, недобросовестные сотрудники компаний все чаще стараются извлечь выгоду из этого. Многие сотрудники компаний считают, что базы данных – это некий «свечной заводик», который сможет приносить стабильный приработок.

Распределение по типам скомпрометированных данных приведено на Рисунке 6. ***По-прежнему основным (доминирующим) типом утекшей информации являются персональные данные.*** Кроме того, на фоне усиления конкурентной борьбы на внутренних и международных рынках росла доля утечек коммерческих секретов и ноу-хау. В то же время случаи утечек платежных данных снижаются: защищённость банковской инфраструктуры растёт, и даже если злоумышленникам удается получить доступ к этой информации, то ее становится все сложнее монетизировать в отличие от ПДн.

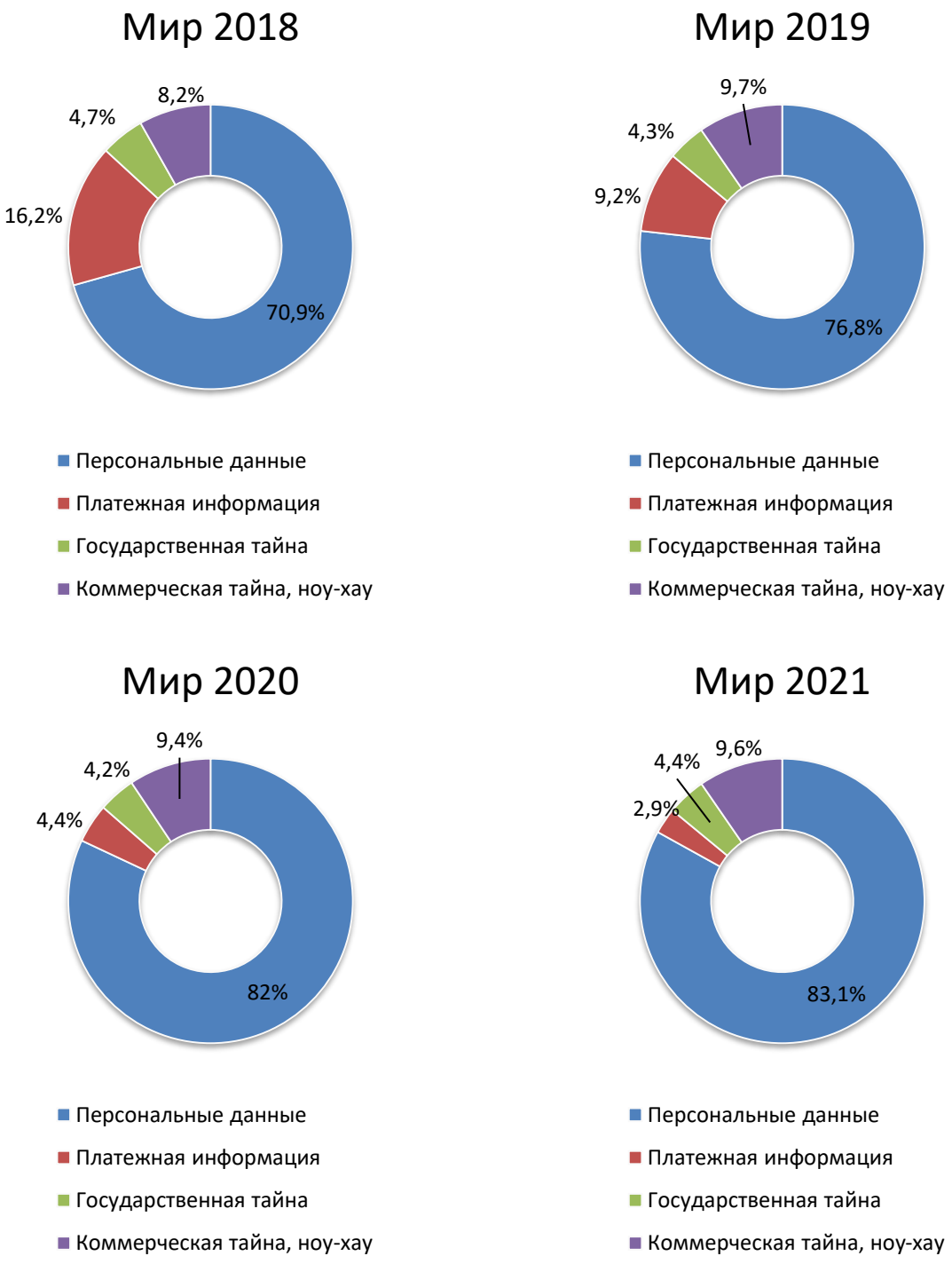


Рисунок 6. Распределение утечек по типам данных: Мир, 2018-2021 гг.

Распределение утечек по внутренним нарушителям представлено на Рисунке 7. Доля непривилегированных сотрудников в 2019 г. снизилась до 81,3%, однако в последующие годы достигла 85%. В то же время в 2018-2020 гг. росла доля утечек по вине руководителей, но в 2021 г. она немного сократилась.

Рисунок 7. Распределение утечек по внутренним виновникам: Мир, 2018-2021 гг.

Распределение утечек по каналам показано на Рисунке 8. Отметим, что в соответствующих выкладках не учтена доля случаев, когда каналы утечек остались неизвестными, и которая ежегодно составляет более 5%.

По прежнему основным остаётся сетевой канал, то есть утечки через подключение корпоративных систем или облачных хранилищ к сети Интернет (см. ниже на рис.8 «Распределение утечек по каналам: Мир, 2018-2021 гг.»).

Доля утечек информации без применения средств автоматизации (компрометация данных в результате кражи или потери бумажных документов, а также в результате кражи или потери средств хранения) за четыре года снизилась более чем в три раза – с 14,1% до 4,5%. Это ещё одно доказательство того, что мир становится всё более цифровым.

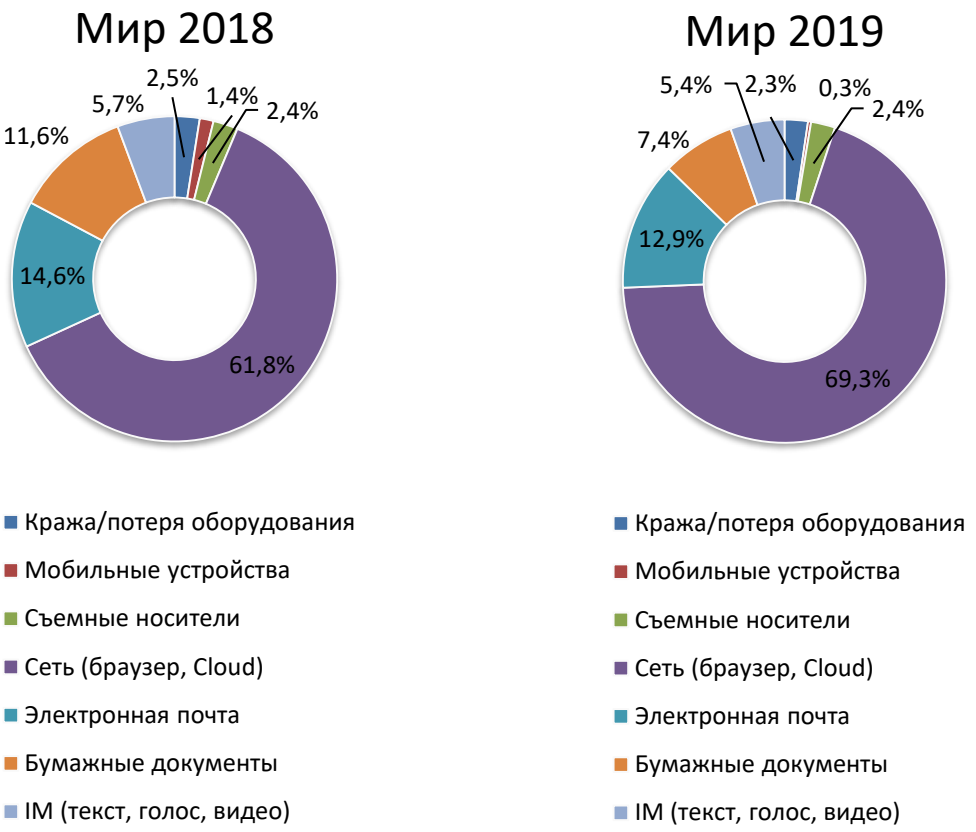
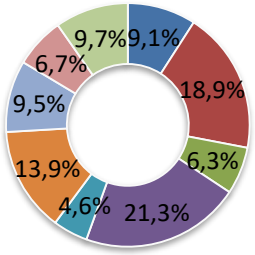


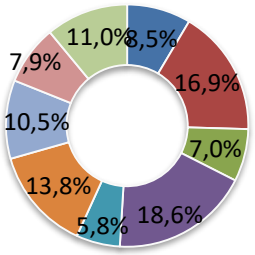
Рисунок 8. Распределение утечек по каналам: Мир, 2018-2021 гг.

Мир 2018



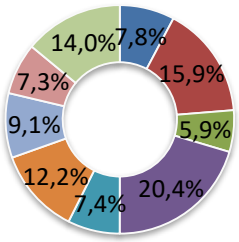
- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

Мир 2019



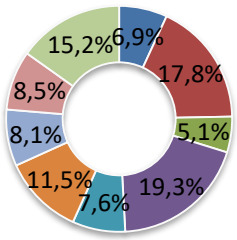
- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

Мир 2020



- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения

Мир 2021



- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения

Рисунок 9. Отраслевое распределение утечек, Мир, 2018-2021 гг.

На Рисунке 9 представлено распределение утечек по отраслям. В последние годы тройку «лидеров» по утечкам стабильно составляют высокотехнологичные компании, организации сфер здравоохранения и госсектора. Обращает на себя внимание то, что сокращается доля утечек в финансовой сфере, при этом стабильно растет доля утечек в промышленности. Также увеличивается доля категории «Другое», куда входит совокупность небольших вертикалей: сфера услуг, туризм, спорт, культура и т.д.

Посмотрим на распределение зарегистрированных в 2021 году утечек по странам (Рисунок 10):

1 место – 41,8% - США.

2 место – 16,8% - Россия.

3 место – 4,9% - Соединенное Королевство Великобритании и Северной Ирландии.

4 место – 3,3% - Канада.

5-6 место – 2,3% - Индия и Япония.

…

9 место – 1,2% - Китай.

Хотя Россия по-прежнему занимает второе после США место по количеству утечек, найденных в открытых источниках, но в 2020 г. количество российских утечек в общем «рейтинге» начало снижаться, а в 2021 г. существенно сократилось (на 40%). Такая ситуация во многом объясняется особенностями формирования карты инцидентов: находясь в России, исследователи могут видеть максимум русскоязычных источников из поисковой выдачи, применяя различные поисковые машины. В то же время вторым ключевым языком поиска в СМИ является английский, а в Дарквебе он основной (преобладающий), поэтому среди найденных случаев доминируют утечки в США, также высока доля опубликованных утечек в других англоязычных странах.

Надо отметить, что стабильными поставщиками новостей об утечках выступают те страны, где развито законодательство о защите информации, прежде всего – персональных данных. Речь в первую очередь идет о США и Евросоюзе, где компании по закону обязаны раскрывать информацию об инцидентах уполномоченным органам, а в случае сокрытия рискуют получить огромные штрафы.

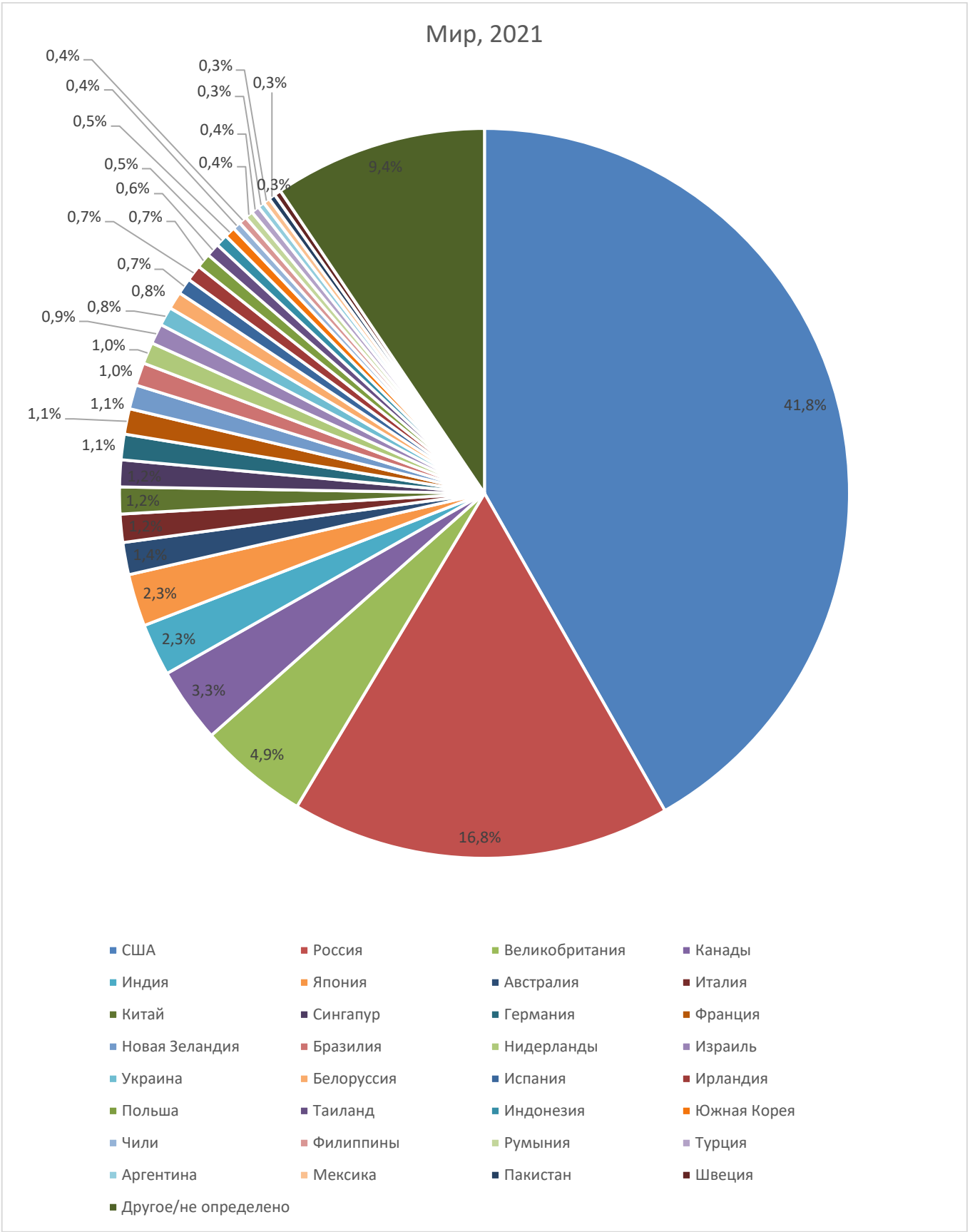


Рисунок 10. Распределение зарегистрированных утечек по странам, 2021 г.

Заключение и выводы

Распространено мнение, что вследствие ускоренной цифровизации и массового перехода на удаленную работу количество утечек должно расти. Но пока мы наблюдаем обратную ситуацию. Причем сокращение идет как в поле известных случаев – опубликованных в СМИ, в отчетах компаний, CERT и т.п., так и при изучении рынка предложений в Дарквебе. Правда, в отдельных исследованиях утверждается, что в США, которые традиционно являются главным поставщиком новостей по теме «data breaches» и «data leaks», продолжается рост количества заявленных утечек – в январе-сентябре 2021 г. на 17% по сравнению с аналогичным периодом прошлого года.

Данные из Даркнета нельзя рассматривать как полностью объективный критерий для аналитики утечек. Главная задача разместившего объявление в подпольном сегменте – продать данные. Отсюда продажи обогащенных баз, то есть наборов данных из нескольких источников (в том числе базы, составленные из утечек прошлых лет). Нередки случаи, когда по сути одна и та же информация продается многократно, также распространены продажи баз по частям (фрагментам). Порой весьма затруднительно определить источник предложенной базы, а также то, равняется ли количество записей в ней сумме записей из конкретной утечки и не является ли это результатом объединения информации из открытых источников (например, в результате так называемого парсинга данных из соцсетей с помощью автоматизированных средств). В 2021 году снизилось количество новых скомпрометированных записей ПДн, тем более, что на подпольных форумах продолжают распространять не потерявшие актуальности обширные базы данных из утечек прошлых лет. Некоторые базы делят на фрагменты и затем обогащают информацией из других источников. То есть необходимо понимать, что количество предложений о продаже информации не равно количеству утечек.

Для злоумышленников также более важным понятием становится ликвидность данных, а не их количество. Поэтому не исключаем, что скоро появятся новые базы, составленные из различных утечек и взаимно обогащенные.

В период пандемии увеличился горизонт инцидента: у компаний больше времени занимает выявление утечки, описание ущерба и его устранение, в результате отодвигается время информирования об утечке регуляторов и потребителей. Как следствие, в системообразующих вертикалях – финансы и госсектор – снижение количества утечек оказалось еще более заметным, чем в целом по отраслевой карте.

Стало больше атак, которые не приводят к утечкам – хакерам достаточно просто зашифровать данные, чтобы получить веский аргумент при шантаже жертвы, позволяющий быстро получить деньги.

Кроме того, значительное количество важной информации стало возможным получать через нелегальное подключение к видеоконференциям, которые стали часто заменять личные встречи. При этом отсутствует необходимость внедрять различные подслушивающие устройства в помещения или подключаться к линиям связи, взламывать корпоративные системы защиты. Важно, что такие случаи практически не выявляются, не публикуются и, соответственно, не попадают в статистику утечек.

Резкое изменение ландшафта угроз ИБ, случившееся в период пандемии, повлекло серьезные сдвиги в формировании структуры утечек.

С точки зрения вектора нарушений вполне ожидаемо в 2021 г. продолжила расти доля утечек по вине внешних нарушителей, то есть хакеров, а также неизвестных лиц из-за пределов корпоративного информационного контура (их действия по определению являются умышленными). Вероятно, существенное снижение утечек внутреннего характера во многом связано с повышенной латентностью соответствующих инцидентов в период пандемии. В ходе широкого перехода на удаленную, а затем гибридную работу, вероятно, в тень стало уходить существенно больше нарушений, в том числе случайного характера, которые можно успешно детектировать при наличии DLP.

Выводы

1. В рассматриваемом периоде (2018-2021 гг.) аномальным по количеству утечек и скомпрометированных записей персональных данных был 2019 год. В результате мошеннические call-центры еще долго «кормились» этими запасами, тем более многие типы ПДн валидны в течение многих лет. Только в конце 2021- начале 2022 гг. стало появляться намного больше объявлений о продаже данных.
2. С 2018 г. неуклонно растет доля утечек по вине внешних нарушителей. Однако, стоит учитывать тот факт, что в ряде стран (США, страны Евросоюза и др.) компании обязаны уведомлять регуляторов об утечках информации. Вероятно, в таком положении компании предпочитают свалить вину на хакеров, нежели проводить расследования внутренних инцидентов. Кроме того, в пандемию могла вырасти латентность внутренних инцидентов. Много утечек ушло в тень из-за трудностей в контроле периметра при удаленной работе, но постепенно некоторые случаи могут раскрываться в будущем.
3. С 58,6% до 82% за четыре года выросла доля утечек умышленного характера. С одной стороны, это может свидетельствовать об относительных успехах, которые компании достигли в борьбе со случайными нарушениями (прежде всего, с помощью DLP). С другой стороны, в пандемийные годы это отчасти может быть связано с повышенной латентностью внутренних нарушений.
4. Среди утечек по вине внутренних нарушителей снижается доля случайных. В 2018 г. она составляла около 65%, а в пандемию сократилась до 48%. Вероятно, здесь можно вести речь как о повышении латентности внутренних, в т.ч. случайных утечек при дистанционной работе (особенно при использовании личных компьютеров для работы с персональными данными), а также о росте привлекательности информационных активов для нарушителей среди персонала.
5. В распределении по типам раскрытых (скомпрометированных) данных стабильно растет доля персональных данных как главного артефакта цифровой эпохи. За четыре года она выросла с 53,7% до 75,3%. ПДн – универсальный тип данных, каждая

единица информации прибрела осязаемую ценность на черном рынке. Доли утечек информации категорий «коммерческая тайна» и «государственная тайна» были относительно стабильны на протяжении 2018-2021 гг. Вместе с тем, в несколько раз упала доля утечек платежной информации (данных банковских карт) – эти сведения в целом надежно защищены, зачастую в руки злоумышленников попадают лишь частичные номера карт, которые невозможно использовать для снятия денег. Эта тенденция продолжает развиваться, например, в марте 2022 г., после того как из России ушли западные платежные системы Visa и Mastercard, информация об эмитированных картах на их основе по сути стала бесполезной – хакеры стали сливать ее буквально за копейки, а то и вовсе предлагать на безвозмездной основе.

6. Хотя Россия по-прежнему занимает второе место по количеству утечек, найденных в открытых источниках, в 2020 г. количество российских утечек в общем «рейтинге» начало снижаться, а в 2021 г. существенно сократилось – на 40%. Вероятно, это можно объяснить как высокой долей латентности внутренних инцидентов (а именно утечки по вине внутренних нарушителей исторически доминируют в нашей стране), так и снижением внимания СМИ к теме утечек на фоне пандемии и последовавшем вале мошенничества с применением «утекших» данными, фишинговых атак и т.д. Снижение количества утечек произошло за счет уменьшения числа внутренних нарушений – количество утечек по вине внешних нарушителей практически не изменилось в 2021 г. Возможно, на это повлиял всплеск интереса к DLP системам с марта 2020 года (начала т.н. «самоизоляции»). В корпоративном сегменте и на удалённых служебных ноутбуках эти системы показали свою эффективность. Возможно, что значительная часть данных, попавших на черный рынок или в открытый доступ за счёт ошибок пользователей, были с личных компьютеров или Интернет-хранилищ, личных почтовых адресов.

7. Продолжает расти стоимость утечки для компаний, допустивших нарушение. Любой инцидент может больно ударить по карману и нанести чувствительный удар по репутации. По данным исследования Ponemon Institute по заказу IBM, одна утечка в 2021 г. в среднем обходилась компании в $4,24 млн. Это на 10% выше, чем в 2019 г.

8. В 2019 г. был зафиксирован резкий всплеск не только количества утечек, но и объема утекших данных, в том числе около 70% записей ПДн (более 10 млрд) стало раскрыто в результате случайных нарушений. В 2020 году количество и доля случайных утечек уменьшились, но превышали 2018 год в 4 раза. В 2021 г. 51% записей (около 4,3 млрд) утекло в результате случайных нарушений (меньше, чем в 2020 году, но в 2,6 раза больше 2018 года).

Год	Умышленные утечки, кол-во записей	Случайные утечки, кол-во записей
2018	5,33 млрд	1,64 млрд
2019	4,87 млрд	10,18 млрд
2020	4,86 млрд	6,84 млрд
2021	4,09 млрд	4,3 млрд

9. За четыре года доля утечек с применением средств автоматизации выросла с 88% до 95%.
10. В 2018-2021 гг. в мире наибольшее количество утечек (в порядке убывания) регистрировалось в следующих отраслях: Высокие технологии, Здравоохранение, Госорганы. В 2018-2020 г. четвертое место занимала сфера Образования, в 2021 г. – Муниципальные органы и организации. В США первое место остаётся за сферой здравоохранения.

Количество утечек в начале 2022 г. вновь начало расти, но главным образом за счет роста хакерской активности. Практически ежедневно поступают сообщения об атаках на известные компании и взломах крупных баз данных. Случившиеся в феврале-марте политические и экономические события серьезно изменят все сферы жизни. Вероятно, антиглобализационные процессы, давно наметившиеся в мире, резко ускорятся, а значит, борьба различных центров влияния спровоцирует не только политические и экономические конфликты, но также новые кибервойны. Хотя основное внимание служб информационной безопасности приковано к мониторингу внешних угроз, ни в коем случае нельзя забывать об опасности, которую для информационных активов потенциально представляют недобросовестные или некомпетентные сотрудники. К тому же, в новой реальности наверняка продолжат усложняться векторы угроз: все чаще речь приходится вести о «гибридных атаках», когда хакеры прибегают к помощи инсайдеров. Компаниям необходимо срочно решать проблему защиты инфраструктуры в условиях комбинированной работы.

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
- VK
- 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. Источником для этой базы являются публичные сообщения[1] о случаях утечек информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления, а также данные из некоторых закрытых и условно-закрытых источников (форумы, чаты, каналы).

В настоящий момент количество записей в базе превышает 20 тысяч.

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

Исследования ЭАЦ, в основном, ориентированы на анализ сообщений об утечках данных на английском и русском языках. Во многом с этим связана большая доля в базе информации об утечках в России и сообщений об утечках из компаний англосаксонских стран и Европы. Для обеспечения и увеличения полноты охвата также используются источники на арабском, японском, немецком, французском, испанском и итальянском языках. В целях данного исследования использовались публикации только на русском языке.

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 каждому сообщению присваивается один из вариантов (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации.

В базу вносятся:

- текст заголовка и сообщения об утечке,
- ссылка на источник сообщения,
- дата публикации сообщения,
- название предприятия (организации, учреждения);
- государство (страна),
- сфера деятельности обладателя информации (отрасль),
- направление деятельности (коммерческая, некоммерческая),
- примерный размер организации (малая, средняя, крупная)[2],
- размер причиненного в результате утечки ущерба[3],
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- субъект[4], непосредственно допустивший утечку.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

- банки, финансовые и страховые компании,
- медицина,

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

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

[3] 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.

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

- 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[5] (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», также в ряде случаев выделяем так называемый «гибридный вектор», когда утечка связана с влиянием как внешних, так и внутренних нарушителей),
- типу нарушителя.

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

Также 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 количество скомпрометированных записей, содержащих только 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.

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

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 и 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.[6] 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),
- обновлённая информация о составе (принадлежности) баз «мега-утечек»,

[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.

- 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).

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:

- утрата услуг, оборудования или устройств;

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

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

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

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
- «Электронная почта» – утечка данных через корпоративную электронную почту.
- «Бумажные документы» – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

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 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]

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 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.