Аналитический отчет

Утечки информации в избранных отраслях, 2021-2023 годы

Оглавление

Только факты

- → В мире за 2023 год количество утечек информации в Промышленности увеличилось на 134%, в Здравоохранении — на 88%, в сфере ИТ/ИБ и Телекоммуникаций — на 35,5%.
- → В России за 2023 год количество утечек информации в Промышленности увеличилось на 4,2%, в Здравоохранении — на 25%. Количество утечек в сфере ИТ/ИБ и Телекоммуникаций, напротив, сократилось — почти на 40%.
- → Сумма долей утечек из Промышленности, Здравоохранения, ИТ/ИБ и Телекоммуникаций в мире составила 33,3%, в России — 25,5%.
- → В мире из компаний ИТ/ИБ и Телекоммуникаций за 2023 год утекло 14,8 млрд записей персональных данных — на 68% больше, чем в 2022 году. В России из компаний этой отрасли в 2022 году утекло 36 млн записей ПДн — в шесть раз меньше, чем в 2022 году.
- → В мировом Здравоохранении за 2023 год утекло 469 млн записей ПДн — на 47% больше, чем в 2022 году. Из российских медучреждений за два года утекло порядка 40 млн записей.
- → В мировой Промышленности среди всех типов скомпрометированной информации доля коммерческой тайны в 2023 году выросла с 38,4% до 66,9%, в российской — с 29,2% до 48%.
- → В Промышленности доля утечек по вине внешних нарушителей составила 97,8% в мире и 92% в России. В Здравоохранении доля утечек по вине внешних нарушителей составила 93% в мире и 75% в России. В сфере ИТ/ИБ и Телекоммуникаций доля утечек по вине внешних нарушителей составила 93,9% в мире и 70,5% в России.

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 (ЭАЦ) подготовил отчет об утечках информации в мире и в России по трем выбранным отраслям: Здравоохранение, ИТ и Телекоммуникации, Промышленность.

Выбор отраслей для исследования обусловлен несколькими мотивами. Так, Здравоохранение вместе с ИТ и Телекоммуникациями играют большую социальную роль, обеспечивая, соответственно, медицинское обслуживание населения и сервисы связи. В то же время Промышленность — это один из локомотивов экономики для многих государств, широкая площадка для внедрения инноваций.

Кроме того, в трех отраслях, определенных исследователями, отмечена весьма интересная динамика инцидентов, связанных с утечками данных. Например, в Промышленности за 2023 год кратно выросло количество утечек в мире, а в России произошел сдержанный рост. Сфера Здравоохранения в мире демонстрирует рост количества утечек информации, при этом в России, после некоторого снижения в 2022 году, их стало больше в 2023 году. В то же время отрасль ИТ и Телекоммуникации показала устойчивый рост количества утечек данных в глобальном масштабе, но в России после существенного увеличения количества утечек в 2022 году последовал спад в 2023 году.

Динамика количества утечек в той или иной отрасли может иметь некоторую зависимость от уровня кибератак. Чем более ценную для хакеров информацию обрабатывают и хранят организации определенной отраслевой категории, тем чаще они страдают от кибератак. Так, согласно отчету Positive Technologies, сфера промышленности в 2023 году вошла в тройку отраслей, которые сильнее всего пострадали от атак с использованием вирусов-шифровальщиков[1]. По данным Statista[2] и IBM, а также Sonicwell, промышленность и вовсе является самой атакуемой отраслью.

ЭАЦ исследовал зарегистрированные в трех выбранных отраслях утечки данных за период 2021-2023 гг. на основе информации, имеющейся в распоряжении аналитиков к началу мая 2024 г. В поле исследования добавлены вновь поступившие сведения об инцидентах, связанных с утечками информации, проведена ревизия случаев, ранее внесенных в базу ЭАЦ, поэтому некоторые результаты отчета имеют незначительные расхождения с данными предыдущих исследований. Это не первый отраслевой отчет об утечках информации в 2024 году: в феврале был выпущен отчёт об утечках в финансовой сфере (Мир и Россия).[3]

---

[1] https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-v-2023-godu-vykupy-vymogatelyam-prevysili-1-milliard-dollarov/#:~:text=%D0%9F%D0%BE%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%BC%20%D0%B8%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20Positive%20Technologies,%D0%B2%D1%8B%D1%81%D0%BE%D0%BA%D0%B8%D0%BC%20%D0%BF%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D0%B5%D0%BC%20%D0%B7%D0%B0%20%D0%B2%D1%81%D1%8E%20%D0%B8%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8E.

[2] https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/#:~:text=In%202023%2C%20manufacturing%20saw%20the,followed%2C%20with%20around%2018%20percent.

[3] https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-finansovom-sektore-za-tri-goda-mir-rossiya

Результаты исследования

Количество утечек информации в мире

В 2023 году экспертно-аналитический центр InfoWatch в мировом масштабе зарегистрировал 1254 утечки информации из промышленных предприятий, что в 2,34 раза (на 134%) больше, чем в 2022 году, и в 13 с лишним раз больше, чем в 2021 году (Рисунок 1). Столь интенсивный рост может быть связан с несколькими факторами. Во-первых, после начала специальной военной операции произошли тектонические изменения в мировой политической системе, и начали формироваться новые центры силы. Поскольку промышленность играет ключевую роль в обеспечении обороны, соответствующие предприятия стали намного чаще служить целями для атак хакерских группировок. Во-вторых, в мире усиливается конкурентная борьба, ноу-хау и стратегические планы тех или иных индустриальных компаний становятся чрезвычайно важной информацией для обеспечения устойчивого развития различных государств в современном мире.

В здравоохранении рост утечек данных более сдержанный: в 2023 году произошло 863 случая, что на 88% больше по сравнению с 2022 годом и на 133,9% больше по сравнению с 2021 годом. По мере развития цифровизации медицина накопила огромные объемы данных о пациентах, и эта информация при отсутствии должного уровня защиты становится легкой мишенью для хакеров и внутренних нарушителей. Персональные данные из систем здравоохранения — довольно ликвидный товар на черном рынке, так как их можно использовать не только для назойливых рекламных предложений и мошенничеств с медицинскими страховками, но и в рамках масштабных фишинговых кампаний, а в некоторых случаях для шантажа.

В мире в отраслевой группе «ИТ/ИБ и Телекоммуникации» отмечено снижение темпов роста количества утечек данных. Если в 2022 году утечек стало больше на 295,5% (почти в 4 раза), то в 2023 году рост составил 35,5%.

Операторам связи, ИТ-компаниям и другим представителям данной отраслевой группы чрезвычайно трудно сдерживать кибератаки, обладая огромными, ликвидными и притягательными для мошенников, конкурентов и спецслужб хранилищами персональных данных, в том числе аутентификационной информации, данными, составляющими тайну связи, различными ноу-хау и коммерческими секретами. Ликвидность обширных пользовательских баз, закрытые финансовые отчеты, стратегические планы развития, сведения о критической информационной инфраструктуре — эта и другая информация пользуется повышенным спросом на черном рынке, поэтому отличается стабильным интересом со стороны злоумышленников. Учитывая меняющуюся ситуацию в мировой политике и экономике, многие компании из сфер ИТ, ИБ и телекоммуникаций в самых разных странах оказались не готовы к защите информации в новых условиях и не устояли перед натиском хакеров и хитроумными схемами внутренних нарушителей, которые, вероятно, намного чаще стали вступать в сговор с внешними злоумышленниками (т.н. гибридный вектор атак).

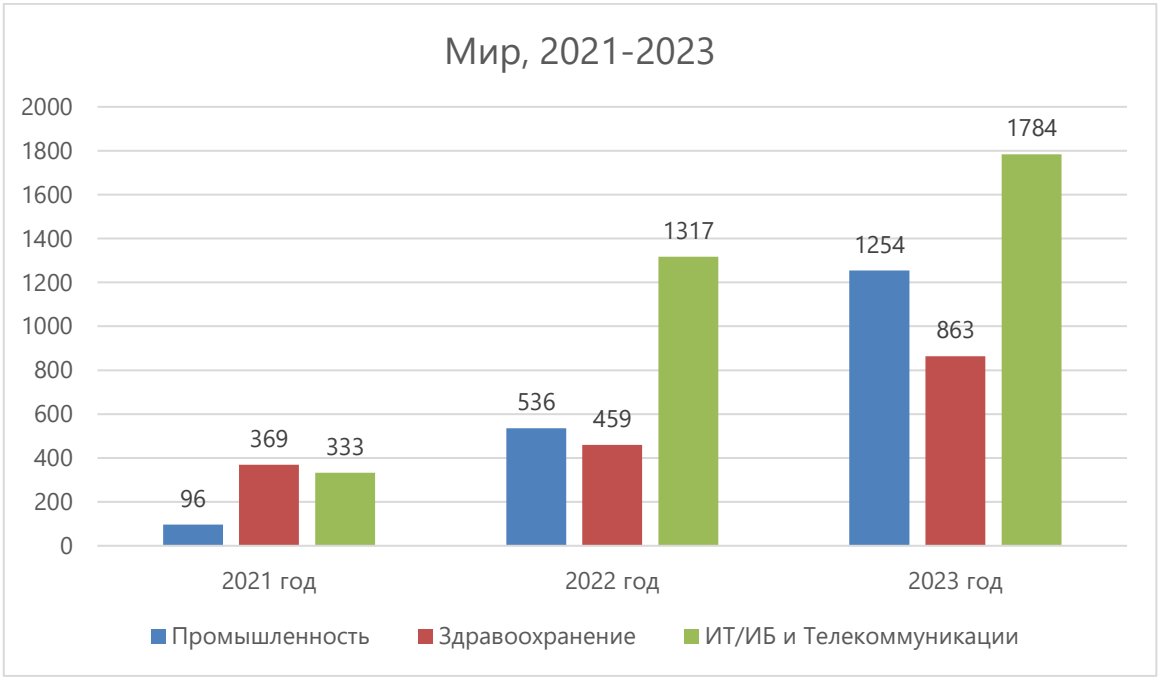

Рисунок 1. Количество утечек информации: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

Количество утечек информации в России

Изменение количества зарегистрированных утечек в трех отраслях российской экономики представлено на Рисунке 2. Как и в глобальном масштабе, в 2022 году произошел резкий рост количества утечек данных среди промышленных предприятий России — в 12 раз. На фоне СВО отечественная индустриальная отрасль столкнулась с высоким давлением со стороны организованных хакерских группировок, причем зачастую данные становятся объектом охоты хактивистов, поддерживающих украинскую сторону конфликта. Но в 2023 году утечек стало больше всего на 4,2%.

В российской сфере здравоохранения в 2023 году зарегистрирован рост количества утечек информации — на 25%, до 20 случаев. Годом ранее количество утечек, напротив, снизилось на 23,8%. На наш взгляд, давление хакеров на российские медучреждения будет возрастать по мере появления крупных централизованных хранилищ данных, развития негосударственных систем здравоохранения и повышения значимости медицинской информации на подпольном рынке данных. Например, в этом году появились мошеннические схемы, связанные с номерами и сроками годности полисов ОМС.

Среди ИТ/ИБ-компаний и телекоммуникационных операторов в России утечек данных в 2023 году стало меньше на 39,7%. Таким образом, российская картина утечек в этой отраслевой категории оказалась зеркальной по сравнению с мировой.

Оправившись от шока 2022 года, связанного с санкционным давлением, уходом ряда ключевых вендоров сфер ИТ и ИБ, потерей привычных ориентиров и экономическими

трудностями, российские компании, вероятно, смогли адаптироваться к стремительно меняющемуся ландшафту угроз, грамотно настроив системы безопасности и начав планомерное замещение зарубежных решений (ПО, ПАК), часть из которого могла иметь (и имела, как позднее выяснилось) серьезные уязвимости.

Рисунок 2. Количество утечек информации: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Доли утечек информации по отраслям

Согласно последним данным ЭАЦ, в глобальном отраслевом распределении утечек в 2023 году доля промышленности по сравнению с 2022 годом выросла почти в 1,5 раза, а по сравнению с 2022 годом более чем вдвое — до 10,7%. Доля здравоохранения после резкого снижения в 2022 году (с 18,6% до 6,4%) вновь увеличилась — до 7,4%. Относительно стабильную долю занимает отрасль «ИТ/ИБ и Телекоммуникации», в 2023 г. она составила 15,2% (Рисунок 3).

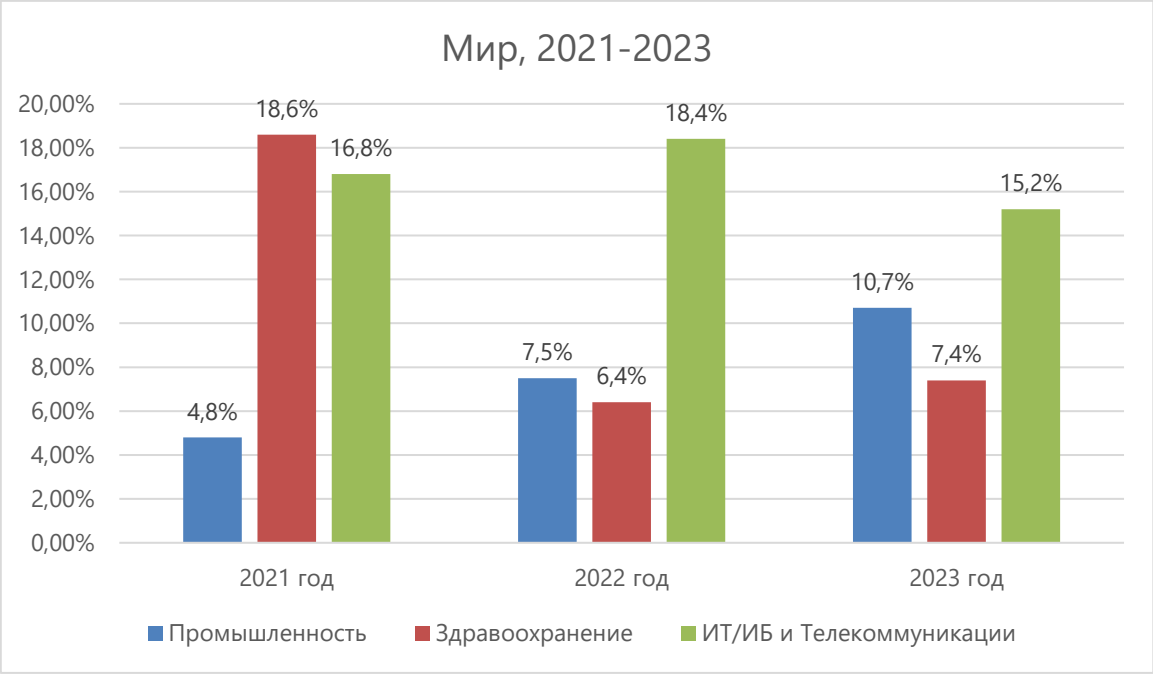

Рисунок 3. Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации: проценты избранных отраслей в общем распределении утечек, Мир, 2021-2023 гг.

В России доля утечек из компаний сферы «ИТ/ИБ и Телекоммуникации» среди других отраслей экономики неуклонно снижается (Рисунок 4). Если в 2021 году она составила 37,5%, в 2022 году — 27,3%, то в 2023 году сократилась до 18,9%. Но, тем не менее, она остаётся одной из основных среди отраслей экономики.[4]

Доля промышленности, напротив, растет — в 2023 году в этой отрасли зарегистрировано 3,7% всех утечек информации их российских компаний и организаций (в 2022 году доля индустриальных компаний составила 3,1%, а в 2021 году только 0,6%).

Колебания демонстрирует доля медицинских учреждений. После падения с 5,9% в 2021 году до 2% в 2022 году она вернулась к росту. В 2023 году доля здравоохранения в российском распределении утечек данных составила 2,9%.

[4] https://www.infowatch.ru/analytics/analitika/rossiya-utechki-informatsii-ogranichennogo-dostupa-2022-2023-gody , страницы 19-20, рис. 13.1, 13.2

Рисунок 4. Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации: проценты избранных отраслей в общем распределении утечек, Россия, 2021-2023 гг.

Утечки — объемы данных по отраслям

В мире ожидаемо доминирующая доля утекших данных приходится на отраслевую категорию «ИТ/ИБ и Телекоммуникации». За 2023 год из совокупности соответствующих компаний утекло более 14,8 млрд записей ПДн (Рисунок 5). Это почти на 68% больше, чем в 2022 году. Огромные базы данных, которые обязаны защищать телекоммуникационные операторы, ИТ-сервисы и соцсети давно стали одними из приоритетных целей для нарушителей. Ситуация, когда защита крупных информационных ресурсов является гораздо более затратным мероприятием, чем их взлом, накладывает на сферу ИТ/ИБ и Телекоммуникаций особую ответственность за сохранение данных своих клиентов. С 2020 года в мире средние расходы на кибербезопасность относительно расходов на ИТ выросли с 8,6% до 11,6%, при этом технологические компании заявляют о крупнейшей доле расходов на ИБ — на уровне 19%[5].

В то же время количество утекших ПДн из промышленных компаний в 2023 году сократилось более чем втрое по сравнению с 2022 годом. Далеко не все индустриальные организации имеют большие базы данных клиентской информации. Кроме того, по данным ЭАЦ, злоумышленников чаще интересуют различные ноу-хау и коммерческие секреты.

[5] https://www.securitymagazine.com/articles/99943-report-shows-cybersecurity-budgets-increased-6-for-2022-2023-cycle

В мировом здравоохранении количество утекших записей ПДн в 2023 году составило 469 млн, что на 47% больше, чем в 2022 году. Скорее всего, по мере роста уровня цифровизации медицины совокупное количество утекшей информации пациентов из этой сферы будет только расти.

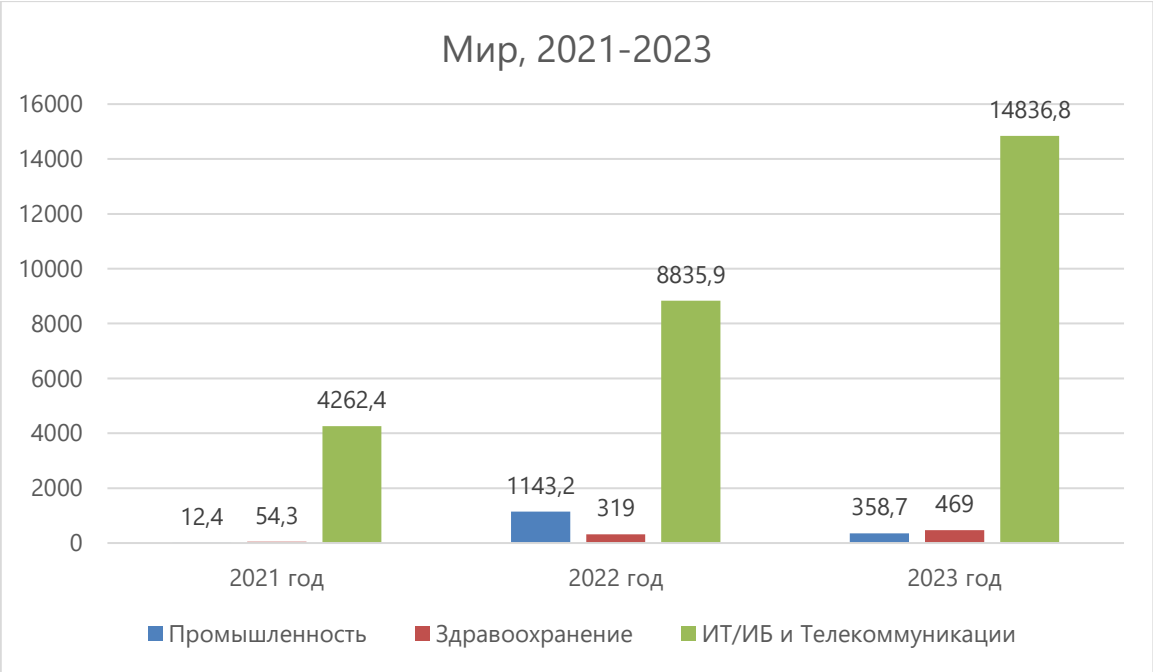

Рисунок 5. Количество скомпрометированных записей ПДн, в млн: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

В российской отраслевой группе «ИТ/ИБ и Телекоммуникации» в 2023 году отмечено не только сокращение количества утечек, но и снижение количества утекших записей ПДн (Рисунок 6). Если в 2022 году было скомпрометировано 228,1 млн записей ПДн, то в 2023 году только 36,1 млн — в шесть с лишним раз меньше. Одной из ключевых отраслей российской экономики удалось избежать большого количества утечек крупных баз данных. Вероятно, залогом этого стала работа самих компаний, планомерные действия Минцифры России и других профильных регуляторов по направлению импортозамещения и других мероприятий, а также проактивная позиция ключевых вендоров в сфере ИБ.

Количество утекших записей ПДн в российской промышленности остается сравнительно небольшим. В 2023 году утекло всего порядка 200 тыс. записей после 3,1 млн годом ранее.

В здравоохранении за два последних года утекло более 40 млн записей. Правда, порядка 30 млн из них (более 75%) зарегистрированы в рамках одной утечки информации — из сети лабораторий «Гемотест».

Рисунок 6. Количество скомпрометированных записей ПДн, млн: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Типы утекших данных[6]

Промышленность

Типы утекших данных из промышленных компаний в мире представлены на Рисунке 7. Доминирующим типом компрометируемых данных выступает информация категории «коммерческая тайна», куда относятся ноу-хау производственных организаций, документы стратегического характера и т.д. Именно на эти данные в первую очередь нацелены нарушители. Ценные сведения, составляющие коммерческую тайну, можно выгодно продать конкурентам пострадавшей компании, организаторам стартапов или использовать как весомый аргумент с целью получения выкупа от жертвы. Не следует забывать и об интересах военно-промышленных корпораций, имеющих серьезные возможности по добыванию интересующих их данных.

[6] Сумма долей может превышать 100%, так как в ряде случаев за одну утечку были скомпрометированы несколько типов данных.

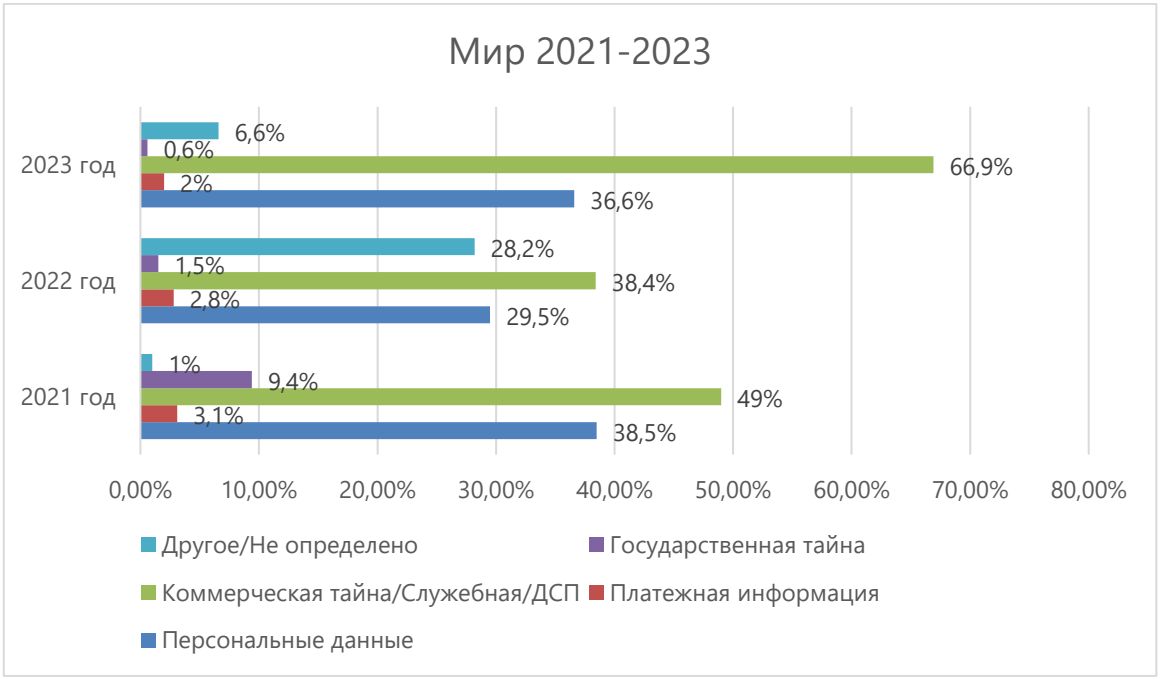

Рисунок 7. Типы утекших данных: Промышленность, Мир, 2021-2023 гг.

Существенно выросла доля утечек коммерческой тайны и в российских промышленных компаниях (Рисунок 8). В 2023 году эта категория присутствовала почти в половине случаев утечек данных из промышленности.

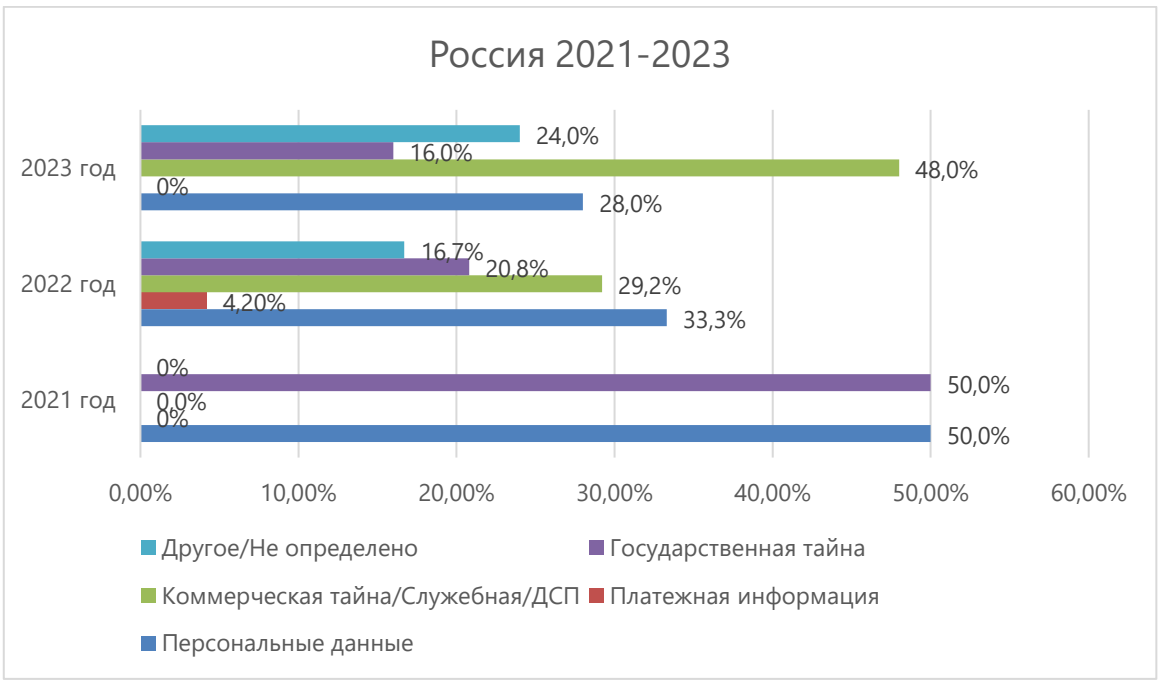

Рисунок 8. Типы утекших данных: Промышленность, Россия, 2021-2023 гг.

Здравоохранение

Коммерческая тайна также стала чаще утекать из учреждений здравоохранения (Рисунок 9). В 2023 году на эту категорию утечек информации пришлось 25,5% случаев. Такая тенденция может быть связана с развитием негосударственной медицины и

ростом конкуренции между частными клиниками в ряде регионов мира. Соответственно, злоумышленники нацеливаются не только на данные пациентов (персональные, врачебную тайну), но и на сведения о бизнесе коммерческих медцентров.

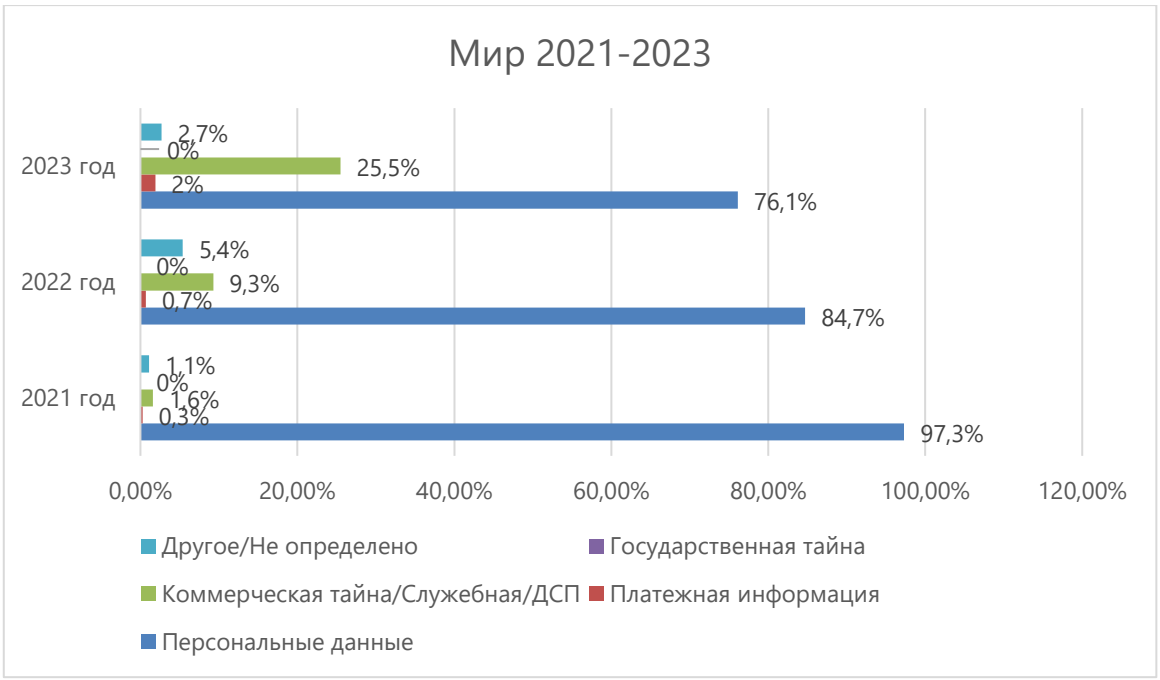

Рисунок 9. Типы утекших данных: Здравоохранение, Мир, 2021-2023 гг.

В российском здравоохранении пока превалируют утечки персональных данных (Рисунок 10). В 2023 году ПДн встречались в 85% случаев.

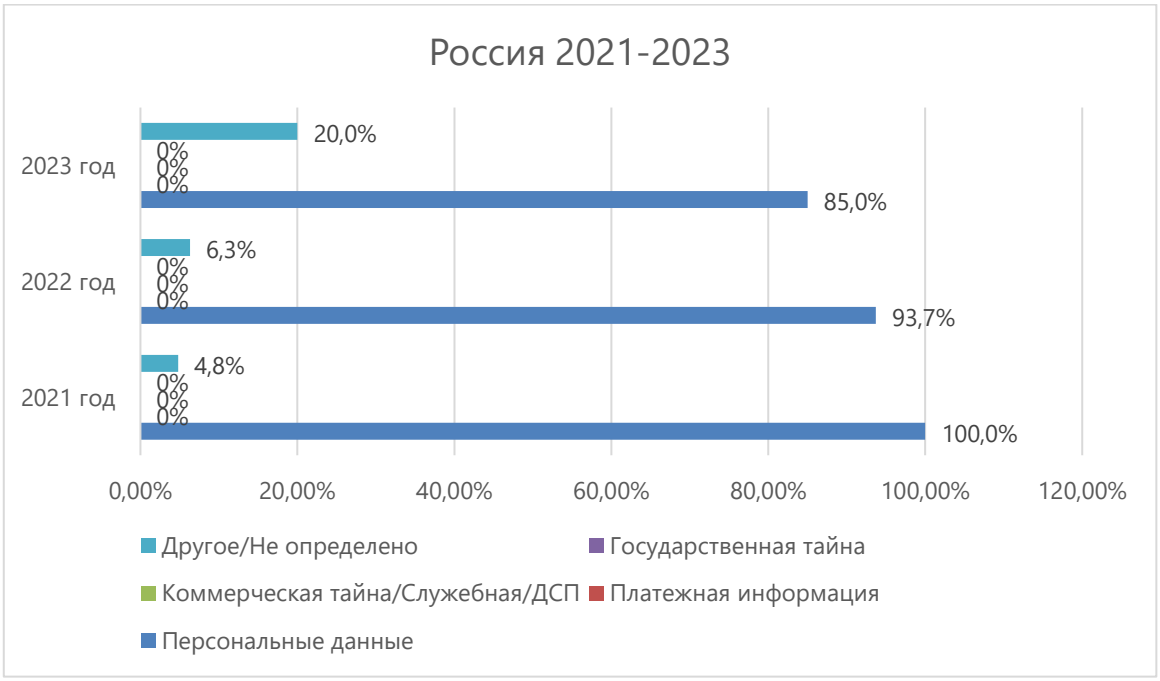

Рисунок 10. Типы утекших данных: Здравоохранение, Россия, 2021-2023 гг.

ИТ/ИБ и Телекоммуникации

В мировом масштабе доля коммерческой тайны выросла и среди утечек в отрасли «ИТ/ИБ и Телекоммуникации». В 2023 году эта категория встречалась почти в четверти утечек данных (Рисунок 11).

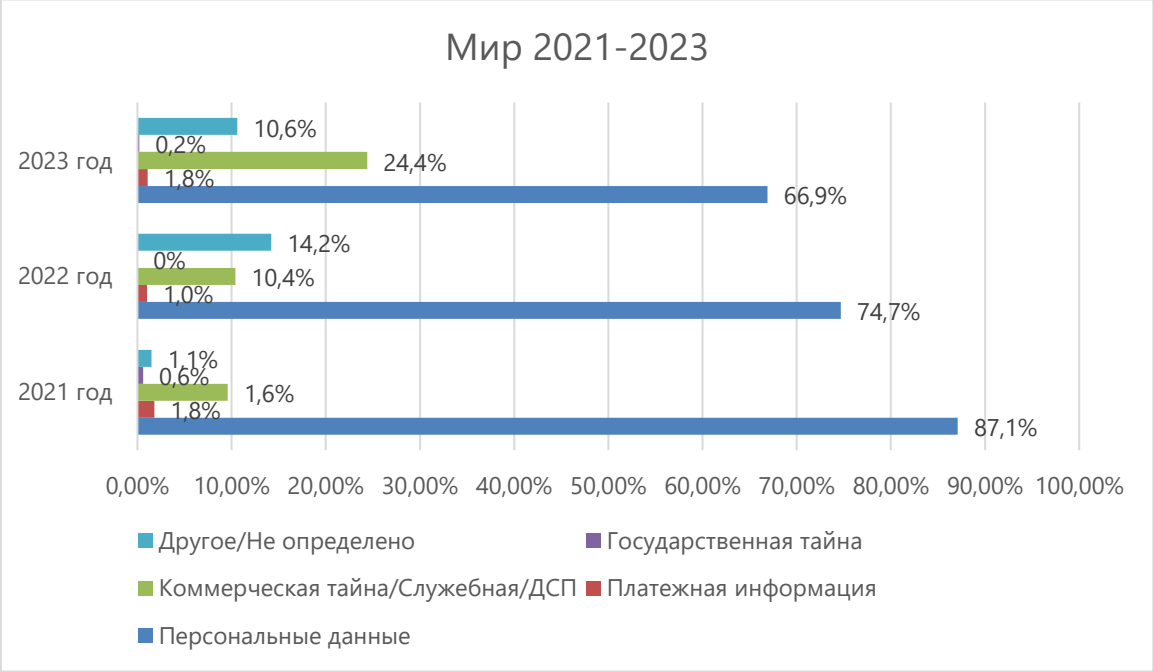

Рисунок 11. Типы утекших данных: ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

В российских компаниях, представляющих ИТ/ИБ и Телекоммуникации, доля утечек, в которых отмечена коммерческая тайна, в 2023 году оказалась примерно вдвое меньше, чем в мире, и составила 13,2% (Рисунок 12).

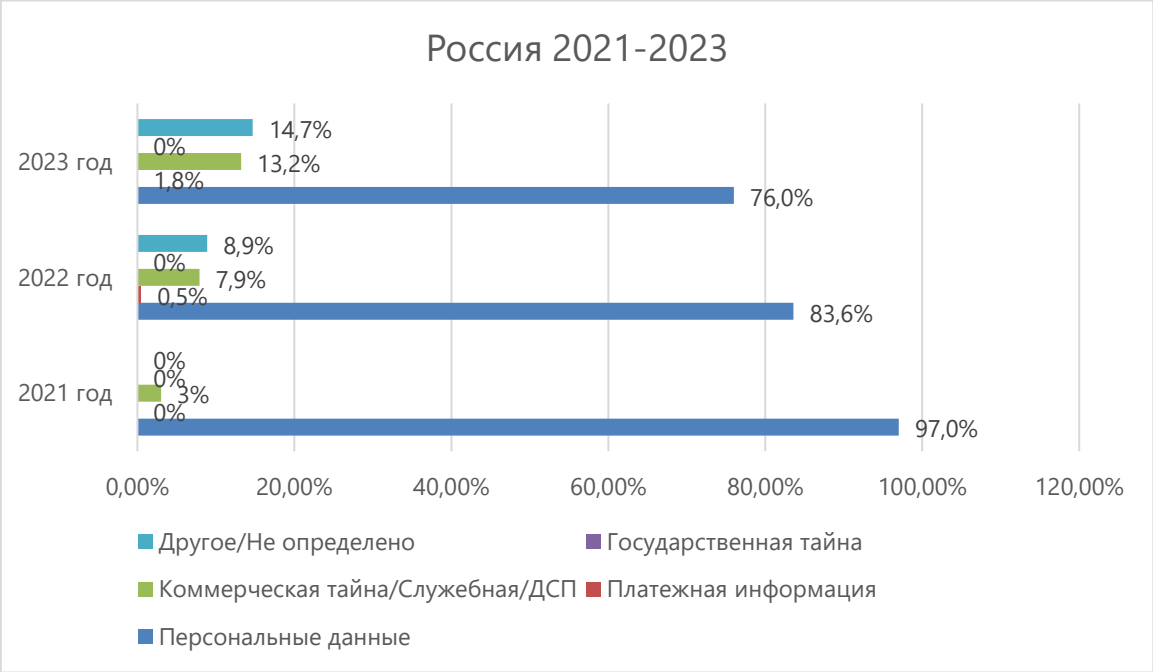

Рисунок12. Типы утекших данных: ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Умышленные утечки

В последние два года доля умышленных утечек из трех рассматриваемых отраслей в мире составила более 90% (Рисунок 13). Правда, в 2023 году во всех трех отраслях она немного снизилась. Высокий процент утечек умышленного характера связан с тремя основными факторами. Во-первых, во время пандемии COVID-19 и на фоне СВО произошли всплески киберпреступности. Особенно во втором случае она на некоторое время стала шоком для многих компаний, тем более, что за многими группировками стоят (по утверждению ряда исследователей) структуры, поддерживаемые государствами (так называемые APT-группировки). Во-вторых, распространение формата удаленной работы привело к усложнению контроля за сотрудниками — несмотря на серьезную эволюцию DLP и других средств противодействия внутренним нарушителям, многие инциденты по вине персонала могут оставаться незамеченными. В-третьих, нередко происходит объединение усилий внешних нарушителей с внутренними: хакеры ищут способы внедрить инсайдера в компании или вступить в сговор с действующими сотрудниками. Иногда «гибридизация» угроз происходит по инициативе самих внутренних нарушителей: обладая знаниями в области архитектуры информационных систем и зная, в какой из них расположены наиболее критичные для бизнеса данные, недобросовестный сотрудник может заручиться поддержкой киберкриминала для «монетизации» своих знаний. Во многих случаях такая «совместная работа» может позволять злоумышленникам действовать скрытно, постепенно скачивая необходимую информацию без следов, а если об утечке становится известно пострадавшей организации, её чаще всего относят к действиям внешних злоумышленников.

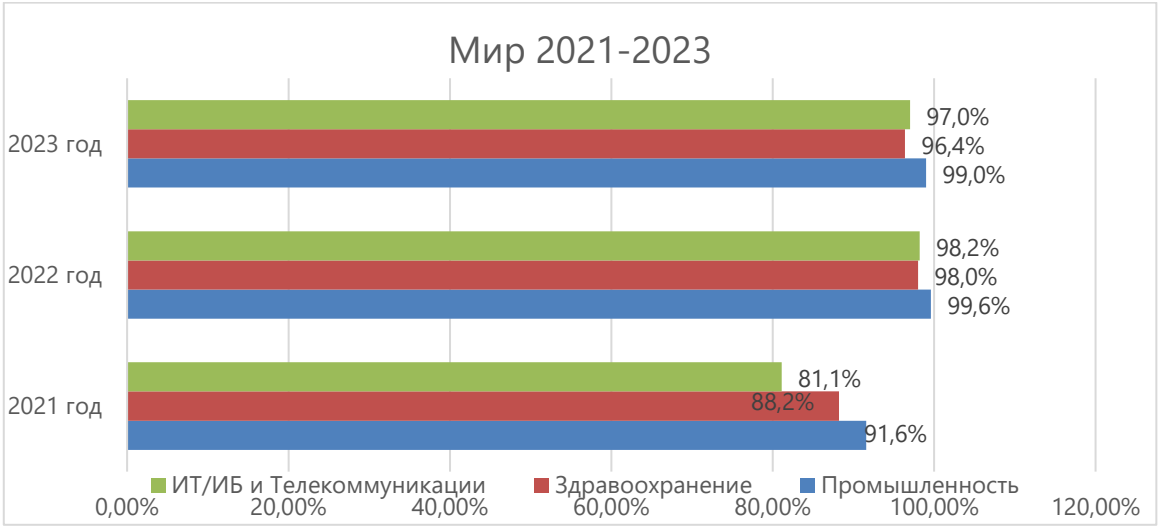

Рисунок 13. Проценты умышленных утечек информации: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

Аналогичные тенденции с точки зрения характера умысла утечек информации прослеживаются и в российских компаниях, представляющих здравоохранение, ИТ/ИБ и телеком, а также промышленность (Рисунок 14).

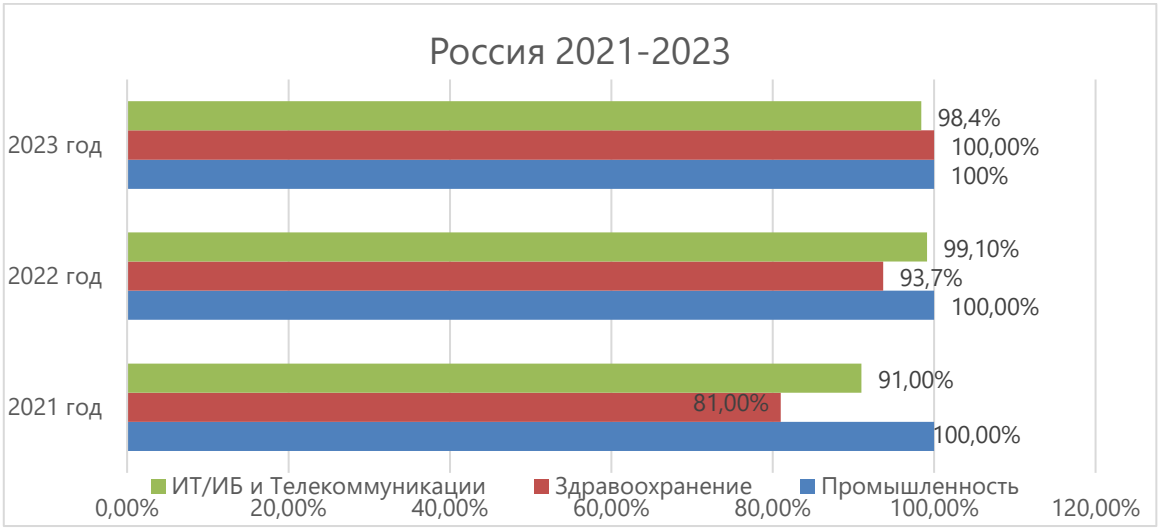

Рисунок 14. Проценты умышленных утечек информации: Промышленность, Здравоохранение, ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Категории виновников утечек информации

Промышленность

В 2023 году среди промышленных компаний в мире в результате действий хакеров произошло 97,8% утечек, в результате действий сотрудников только 1,8% (Рисунок 15).

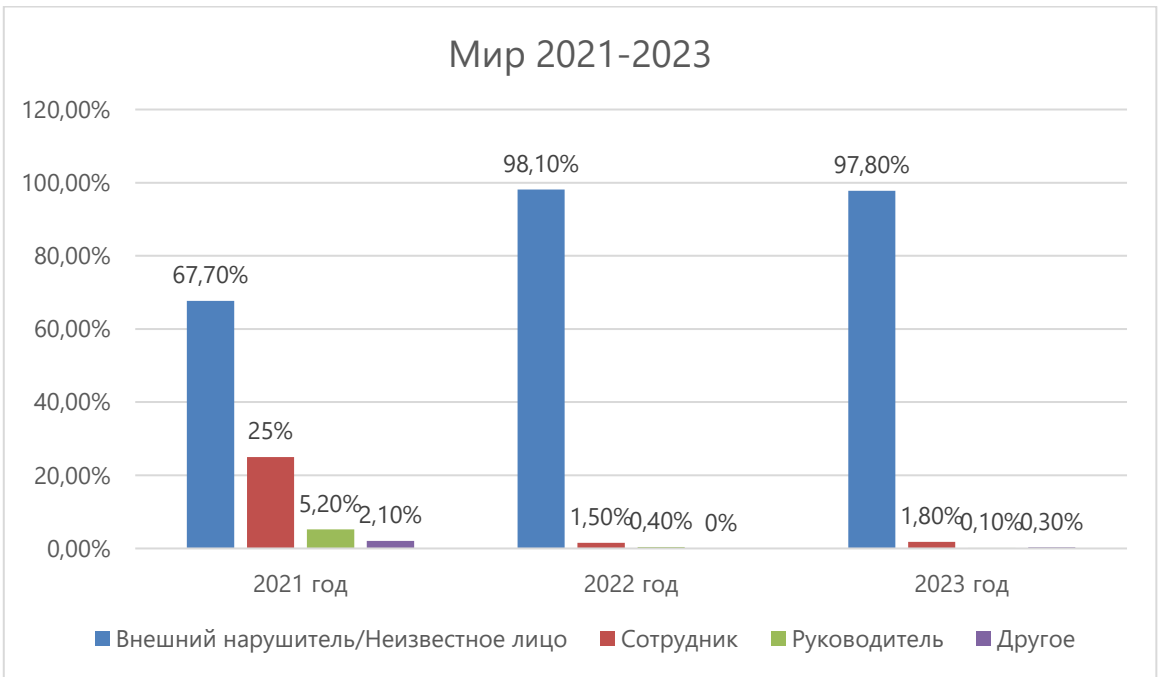

Рисунок 15. Категории виновников утечек информации: Промышленность, Мир, 2021-2023 гг.

В российской промышленности доля сотрудников среди виновников утечек в 2023 году составила 8% (Рисунок 16). В целом российские индустриальные предприятия испытывают повышенное давление со стороны киберпреступности, поэтому именно

защита от внешних угроз, включая обеспечение безопасности АСУ ТП, скорее всего, будет приоритетом отечественной промышленности на ближайшие годы.

Рисунок 16. Категории виновников утечек информации: Промышленность, Россия, 2021-2023 гг.

Здравоохранение

Среди учреждений здравоохранения в глобальном масштабе доля внешних нарушителей среди виновников утечек в 2023 году составила 93%, а доля сотрудников — 6,3% (Рисунок 17).

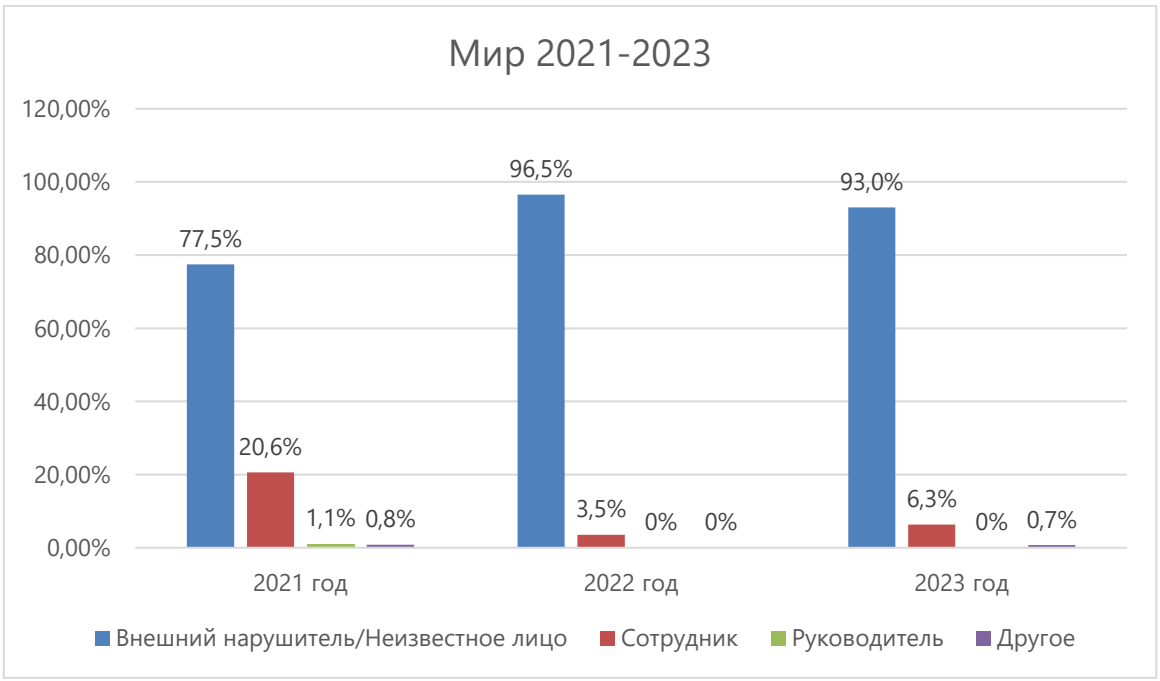

Рисунок 17. Категории виновников утечек информации: Здравоохранение, Мир, 2021-2023 гг.

В российской медицине заметную роль среди нарушителей по-прежнему играют сотрудники. В 2023 году их доля составила 25% (Рисунок 18). Из позитивных тенденций в этой отрасли можно отметить то, что в ней практически перестали встречаться утечки по халатности персонала (пациенту распечатали рецепт на бумаге с персональными данными других людей, медицинские карты выбросили на помойку и т.д.). Это связано не только с сокращением бумажного документооборота, но и с повышением уровня культуры сотрудников при работе с ПДн.

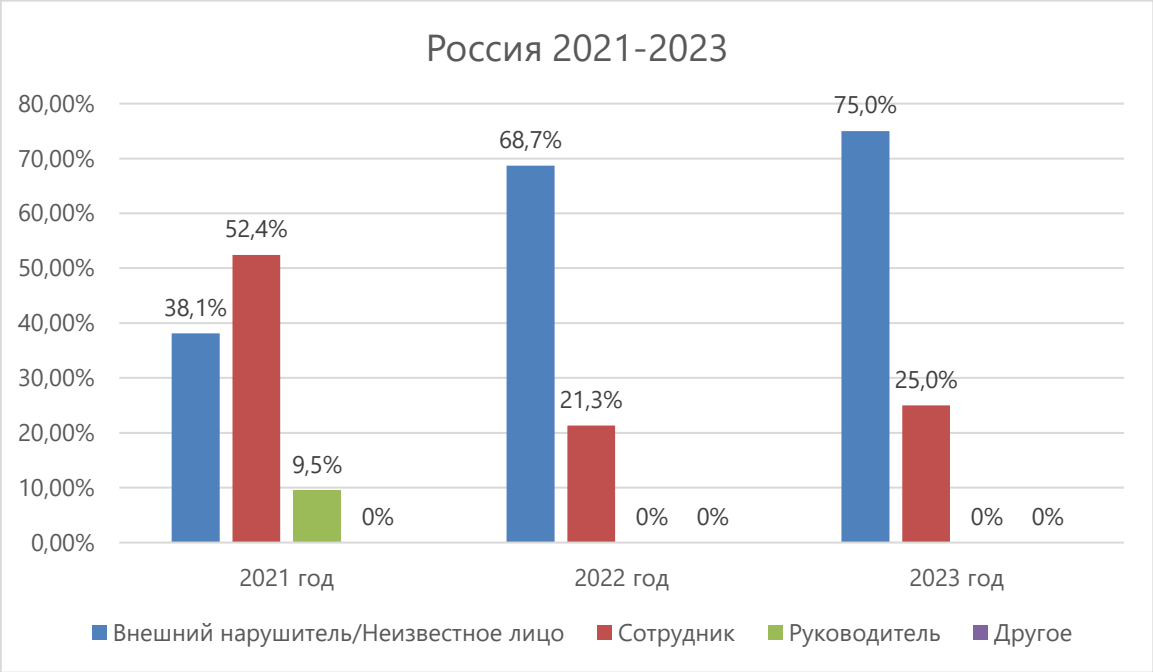

Рисунок 18. Категории виновников утечек информации: Здравоохранение, Россия, 2021-2023 гг.

ИТ/ИБ и Телекоммуникации

В мировой сфере ИТ/ИБ и Телекоммуникаций доля хакеров среди нарушителей за последнее время выросла в два с лишним раза и составила 93,9% в 2023 году (Рисунок 19). Доля сотрудников, которая преобладала еще в 2021 году, в течение двух лет сократилась до 5,2%. (сократилась и по количеству утечек за счет сотрудников, не только доля) Судя по всему, компании отрасли стали лучше справляться с внутренними угрозами, прежде всего в плане предупреждения мошенничеств со стороны менеджеров операторских компаний. Хотя в абсолютном выражении утечек по вине персонала стало ненамного меньше.

Сектор высоких технологий, к которому относятся организации отраслей ИТ/ИБ и Телекоммуникации, уже много лет занимает весомую долю в общей статистике утечек информации ограниченного доступа. Эти организации являются локомотивами цифровизации, разрабатывая и внедряя современные технологии, обеспечивая услугами связи граждан, государство и бизнес, в том числе храня огромные массивы

аутентификационной информации. Поэтому данные из сферы ИТ/ИБ и Телекоммуникаций традиционно пользуются повышенным спросом на черном рынке. Вместе с тем, сотрудники данной сферы как новаторы часто склонны к риску, применению передовых, но не проверенных с точки зрения отсутствия уязвимостей решений, поэтому они часто могут находиться в зоне повышенного риска против хитроумных атак. Помимо этого, телекоммуникационные и ИТ/ИБ компании зачастую отличаются довольно отрытой корпоративной культурой. С одной стороны, это способствует раскрытию потенциала сотрудников, стимулирует развитие новых технологий, а с другой, не всегда способствует обеспечению задач защиты информации, так как в открытой ИТ-среде, где часто принято делиться своими разработками (например, open-source проекты), проще действовать инсайдерам. В результате компании из сферы высоких технологий имеют повышенную площадь поверхности атак, то есть существует довольно много возможностей похищения информации для преступников.

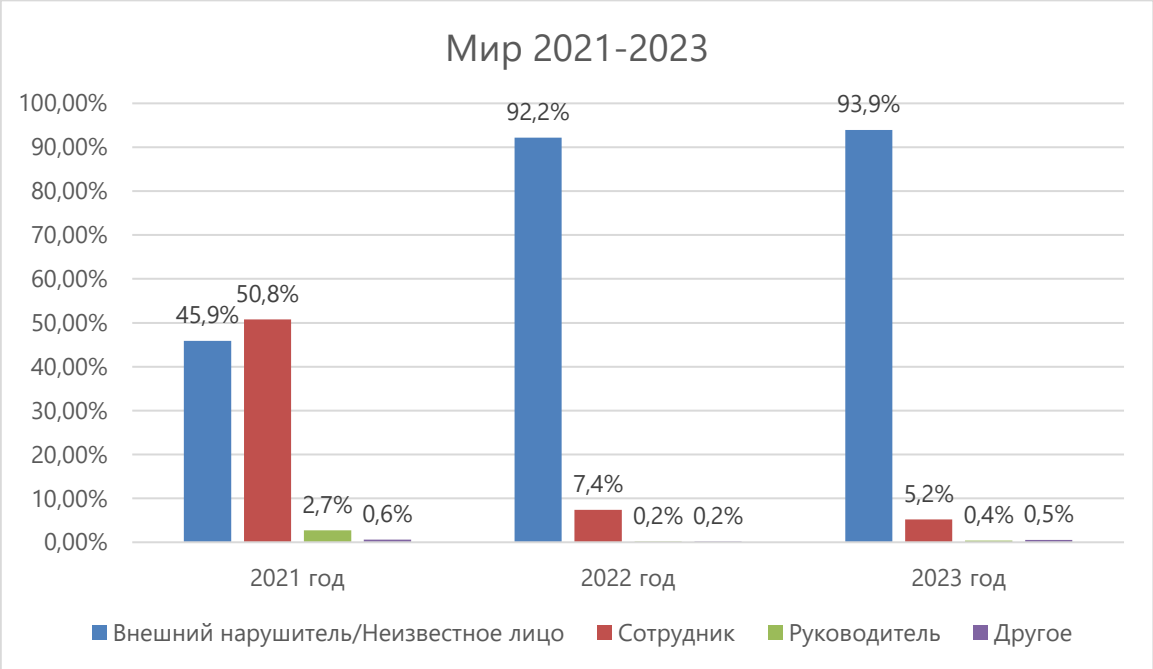

Рисунок 19. Категории виновников утечек информации: ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

Информационные активы направления «ИТ/ИБ и Телекоммуникации» в России пока довольно сильно страдают от действий сотрудников. Доля этой категории нарушителей в 2023 году составила 27,1% (Рисунок 20).

Рисунок 20. Категории виновников утечек информации: ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Каналы утечки информации

Промышленность

В мировой промышленности 98% утечек в 2023 году произошло через Сеть (Рисунок 21).

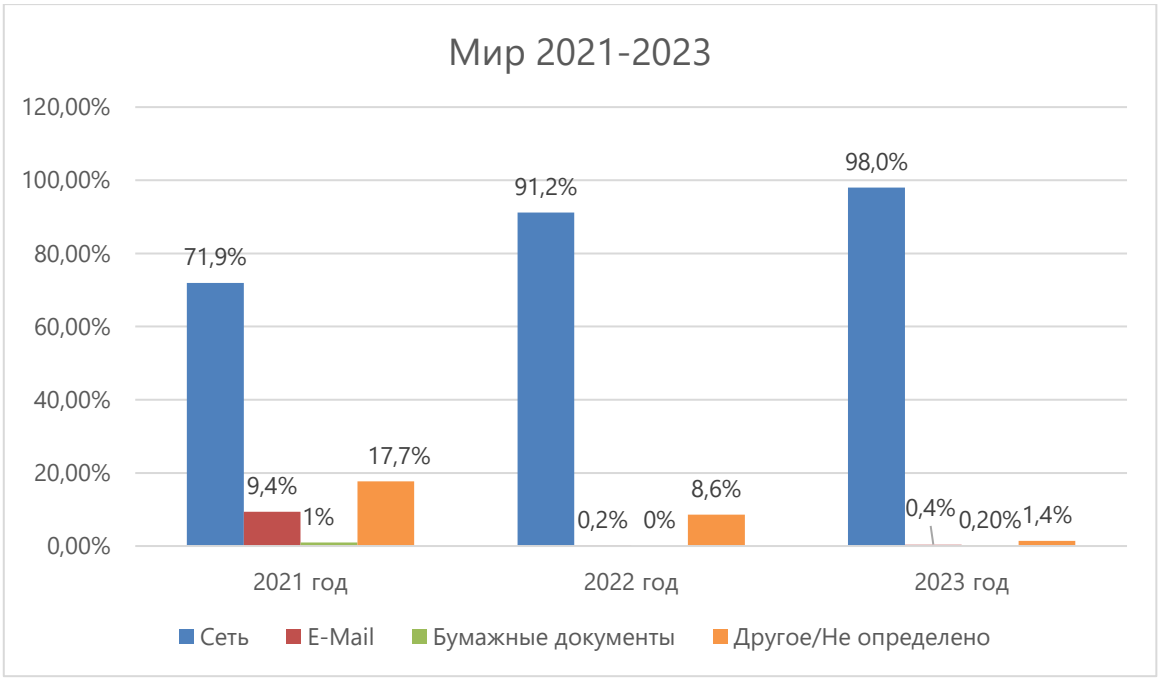

Рисунок 21. Каналы утечек информации: Промышленность, Мир, 2021-2023 гг.

Среди российских индустриальных компаний доля утечек через Сеть составила не менее 84% (Рисунок 22).

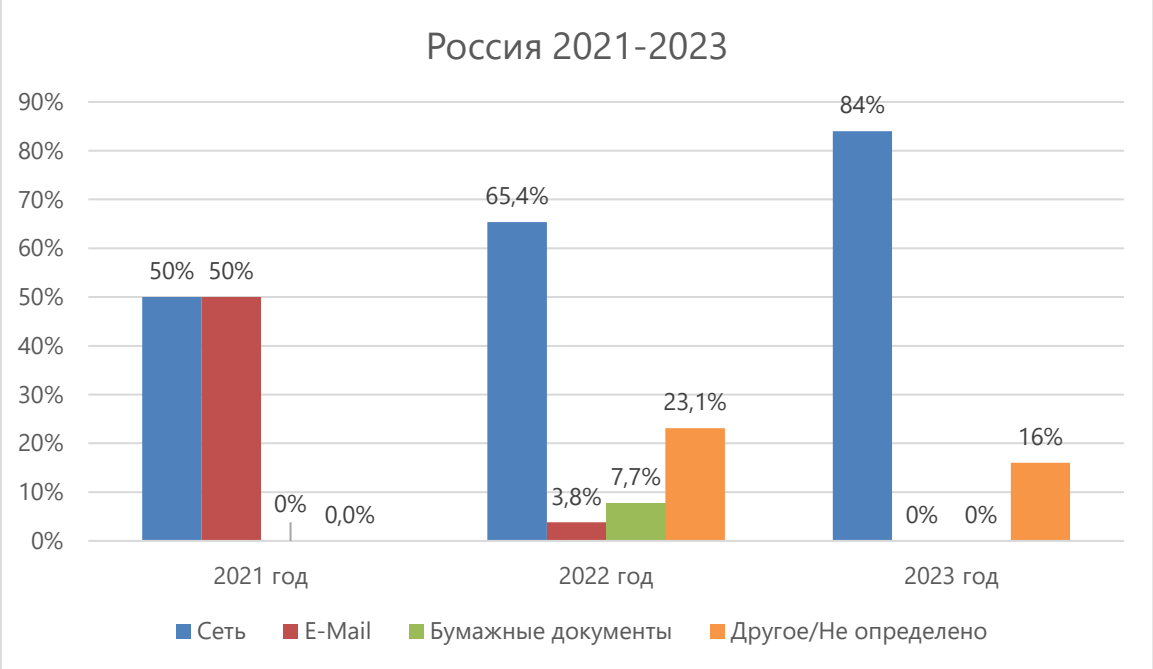

Рисунок 22. Каналы утечек информации: Промышленность, Россия, 2021-2023 гг.

Здравоохранение

В мировом здравоохранении доля утечек информации через Сеть составила без малого 90% (Рисунок 23). Заметные доли в этой отрасли продолжают занимать такие каналы, как электронная почта и бумажные документы.

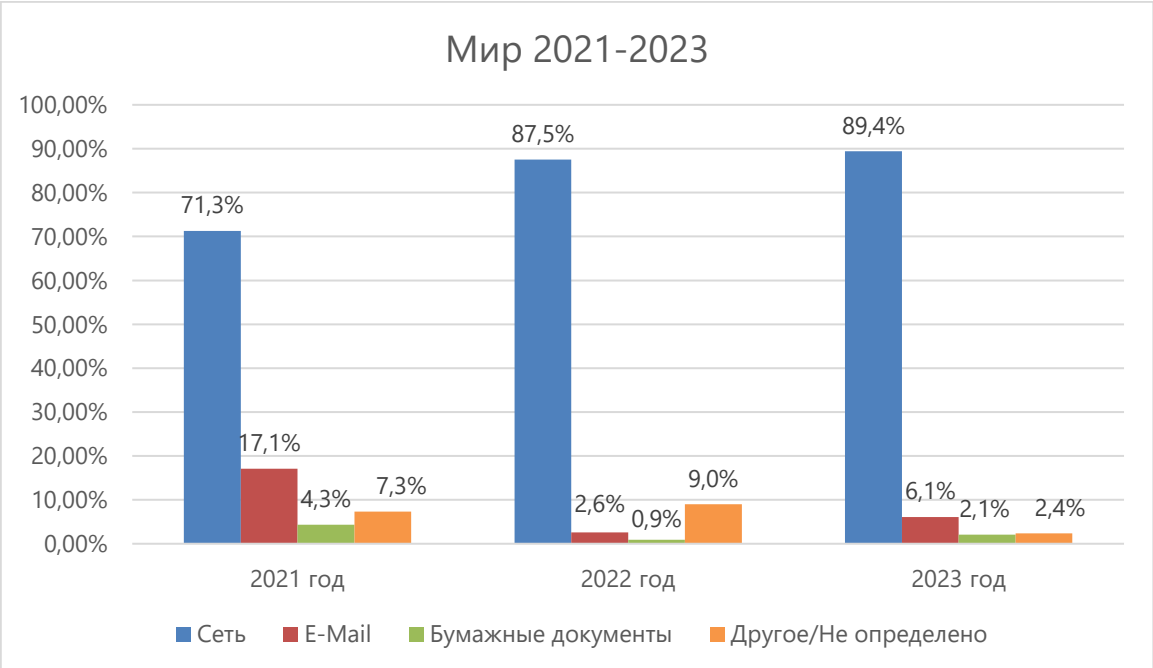

Рисунок 23. Каналы утечек информации: Здравоохранение, Мир, 2021-2023 гг.

В России среди медицинских организаций за 2023 год впервые не было зарегистрировано ни одной утечки посредством кражи или потери бумажных носителей (Рисунок 24).

Рисунок 24. Каналы утечек информации: Здравоохранение, Россия, 2021-2023 гг.

ИТ/ИБ и Телекоммуникации

Среди компаний из отраслевой категории «ИТ/ИБ и Телекоммуникации» в мире также превалирует сетевой канал (Рисунок 25).

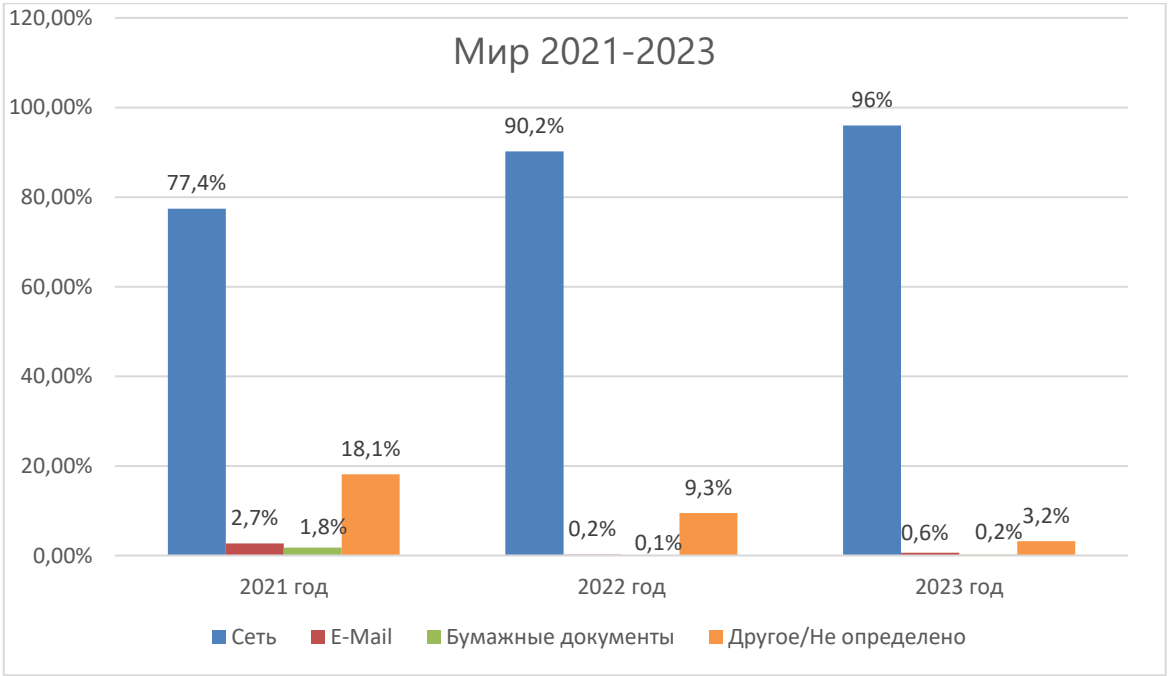

Рисунок 25. Каналы утечек информации: ИТ/ИБ и Телекоммуникации, Мир, 2021-2023 гг.

В России около 80% из сферы ИТ/ИБ и телекоммуникаций за 2023 год произошли через Сеть (Рисунок 26).

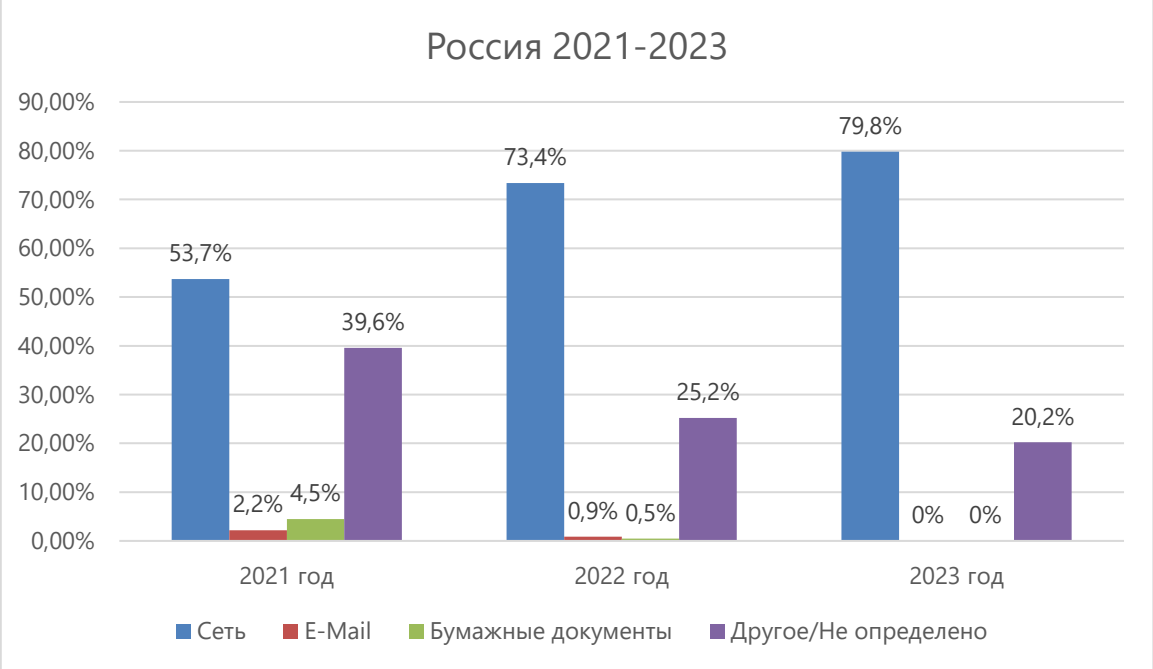

Рисунок 26. Каналы утечек информации: ИТ/ИБ и Телекоммуникации, Россия, 2021-2023 гг.

Заключение

Изучение утечек данных в отраслевом разрезе позволяет получить более полное представление о характере угроз информационным активам в той или иной вертикали. Исследование ЭАЦ показало, что в разных отраслях есть свои тенденции формирования картины утечек. Среди трех выбранных отраслей в мире наибольшие темпы роста количества утечек данных демонстрирует промышленность, а наименьшие — здравоохранение. В России среди промышленных компаний и учреждений здравоохранения в последнее время рост количества утечек сравнительно небольшой, а сфера ИТ/ИБ и Телекоммуникаций даже смогла переломить негативный тренд, и утечек в прошлом году в ней стало меньше почти на 40%.

За 2023 год в сумме отрасли Здравоохранение, ИТ/ИБ и телекоммуникации, а также Промышленность составляют треть утечек информации в мире и более четверти — в России. Из мировых компаний сферы «ИТ/ИБ и Телекоммуникации» утекает наибольшая доля записей ПДн, в то же время в российском масштабе соответствующие организации более успешно противостоят угрозам и практически не подвергались утечкам крупных баз данных в 2023 году.

Промышленная отрасль в мире наиболее часто подвергается утечкам информации категории «коммерческая тайна» (2/3 всех инцидентов). В России эта категория также стала намного чаще фигурировать в сообщениях об утечках информации из

индустриальных компаний. В то же время среди учреждений здравоохранения в основном встречаются утечки персональных данных.

Хакеры и другие категории злоумышленников как в России, так и в целом в мире все чаще объектом охоты выбирают интеллектуальную собственность и другие коммерческие секреты организаций. Утечка такого рода данных может лишить компанию конкурентных преимуществ, если похищенная информация попадет в руки конкурентов. Опережающий рост количества утечек коммерческой тайны по сравнению с ПДн — весьма опасная мировая тенденция. Она может быть вызвана новым витком торговых войн, перераспределением акцентов среди хакерских группировок и постепенным насыщением подпольного рынка ПДн.

Основной угрозой для трёх рассмотренных в отчёте отраслей в России выступают внешние злоумышленники — как операторы вирусов-вымогателей, стремящиеся завладеть ликвидными данными и/или получить выкуп, так и группы хактивистов, которые в условиях СВО рассматривают кражу данных в контексте вооруженного конфликта и готовы сливать данные бесплатно, чтобы заявить о своей позиции.

Мероприятия по укреплению защиты от внешних угроз не означают снижения внимания к внутренним нарушителям. Инсайдерские угрозы становится все сложнее обнаружить в рамках распространения ИИ и других современных технологий, при развитии практики гибридной работы. В современных условиях это направление требует сложных, многогранных подходов, включающих обучение сотрудников, внедрение передовых технологий мониторинга, включая контроль привилегированных пользователей и регулярную ревизию парка учетных записей, а также использование современных инструментов DLP для предотвращения утечек различного характера.

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

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

«Методика сбора, обработки и анализа сведений об утечках охраняемой законом информации. Версия от 28.02.2023 г.»

Настоящим свидетельством Акционерное общество «Национальный Реестр интеллектуальной собственности» подтверждает, что 05.04.2023 г. файл «Методика сбора, обработки и анализа сведений об утечках охраняемой законом информации. Версия от 28.02.2023 г.» по заявлению: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЛАБОРАТОРИЯ ИНФОВОТЧ" (ОГРН 1087746543367, ИНН 7734583888), зашифрован и помещен в виртуальную ячейку АПК НРИС.

Объект интеллектуальной собственности может быть предоставлен Депоненту на основании заявления или по запросу органов государственной власти.