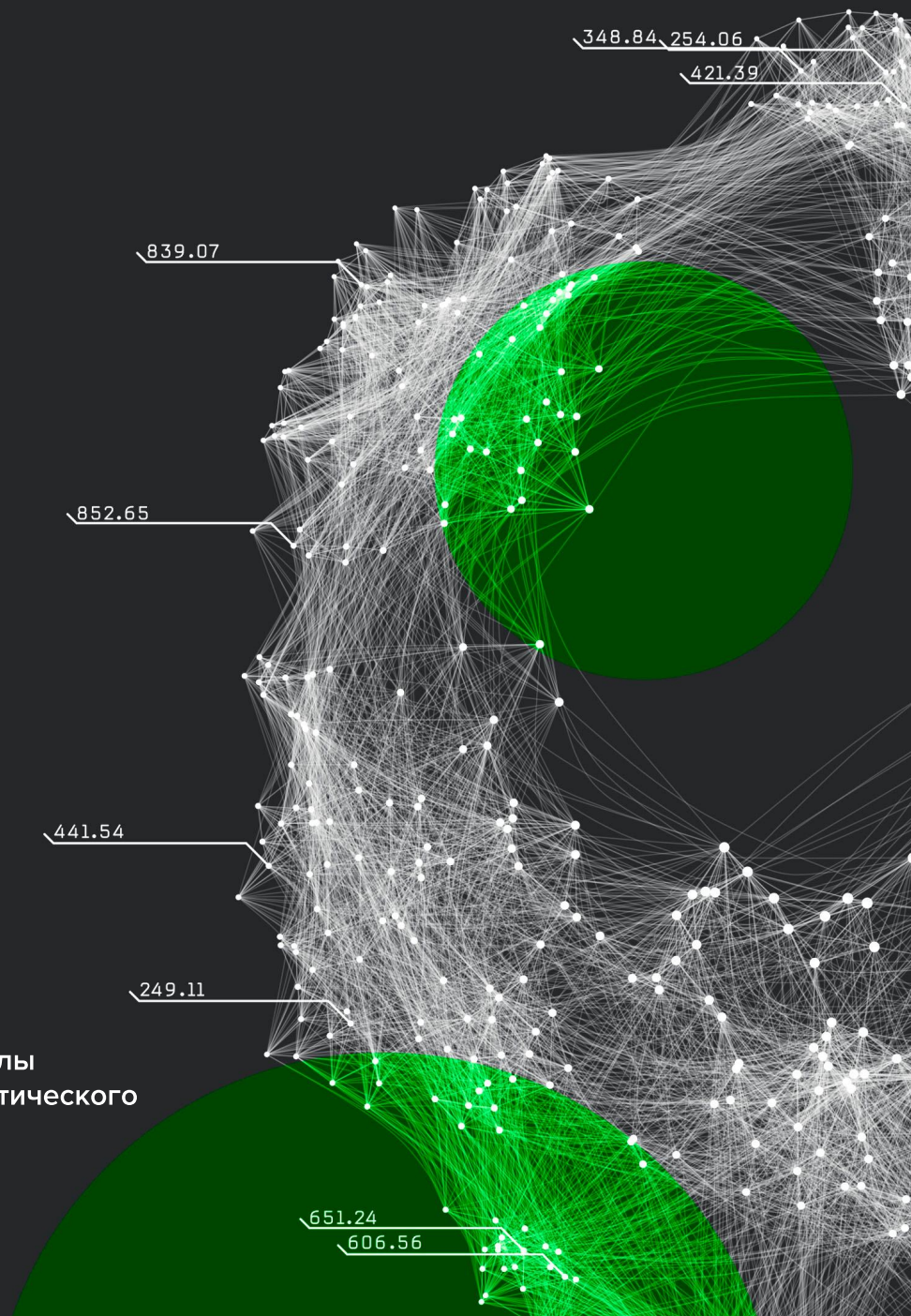
INFOWATCH®

аналитический отчет

УТЕЧКИ ИНФОРМАЦИИ В МИРЕ И РОССИИ ЗА ПЕРВОЕ ПОЛУГОДИЕ 2024 ГОДА



Читайте материалы экспертно-аналитического центра InfoWatch

Оглавление

Только факты

В России утечек информации стало больше на ↑ **10%**

Утечек информации в мире стало **меньше** в основном за счет снижения количества зарегистрированных инцидентов в США

Количество утекших записей персональных данных в России за I полугодие составило почти **1 млрд**

Крупных баз в первом полугодии 2024 года утекло **на треть меньше** ↓, чем в первом полугодии 2023 года.

На одну утечку информации в мире в среднем приходится **2,52 млн** записей ПДн, в России — **2,38 млн**

Доля **умышленных нарушений** среди утечек информации в России составила более **99%**

В I полугодии 2024 года заметно **выросли доли утечек** в торговле и промышленности

В России почти **вдвое выросла доля утечек** гостайны

Более половины утечек информации в России случились **в сфере малого бизнеса**

Сокращения

GDPR	General Data Protection Regulation (Регламент Евросоюза о ПДн 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) представил отчет по результатам традиционного исследования утечек информации за первое полугодие календарного года.

В отчете рассмотрена динамика количества утечек информации в сравнении с предшествующими периодами. Аналитики объясняют, почему в мире зарегистрированных инцидентов, связанных с компрометацией данных, стало меньше, а в России, напротив, количество таких инцидентов выросло. Проведенное исследование также позволило сделать выводы о соотношении количества утечек информации в различных отраслях и оценить, насколько изменились доли утечек в компаниях разного размера.

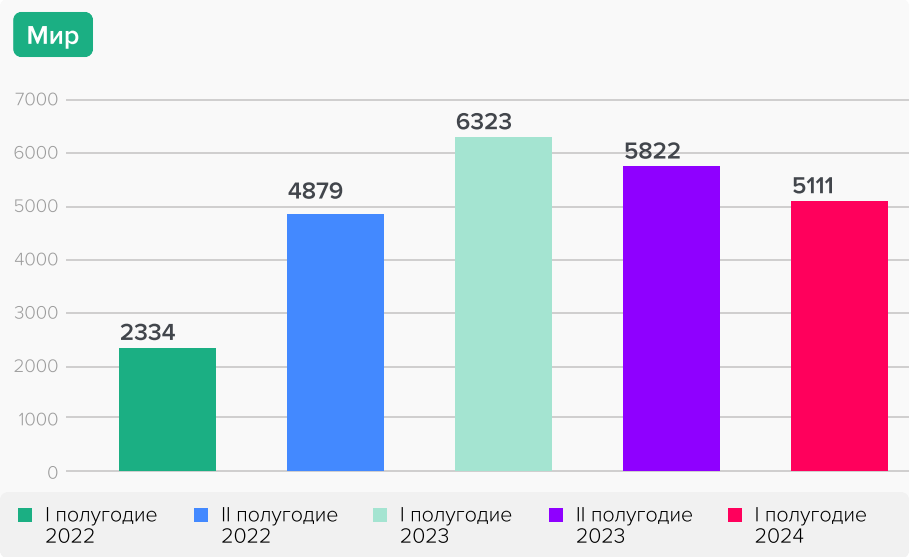
Отчет будет полезен акционерам и директорам компаний, руководителям и специалистам по ИБ, ЭБ и ИТ, а также всем, кто интересуется темой защиты информации в государственных органах и коммерческих компаниях.

Результаты исследования

Количество утечек в мире сократилось на 19%, а в России выросло на 10%

В первом полугодии 2024 года ЭАЦ ГК InfoWatch зарегистрировал* 5111 утечек конфиденциальной информации по всему миру (см. Методику). Это на 19,2% меньше, чем в первом полугодии 2023 года, в котором произошло 6323 случая компрометации данных из коммерческих компаний и госсектора (Рисунок 1). При этом количество утечек информации в первой половине 2024 года оказалось в два с лишним раза (на 119%) больше, чем за аналогичный период 2022 года, когда по данным экспертно-аналитического центра было зарегистрировано 2334 утечки информации.

Рисунок 1. Количество утечек информации: Мир, I полугодие 2022 г. - г., I полугодие 2024 г.



Несмотря на некоторое снижение в I полугодии 2024 года количества инцидентов, повлекших утечки информации, эпоха массовой компрометации данных продолжается. Ежедневно регистрируются десятки случаев компрометации различных сведений конфиденциального характера. На наш взгляд, снижение количества утечек информации в мире, вполне вероятно, носит временный характер и связано с относительными успехами по укреплению систем защиты в отдельных странах и отраслях, а также с переоценкой злоумышленниками своих приоритетов и возможностей. Скорее всего, далеко не все факты об утечках, случившихся в первой половине года, стали известны к моменту выхода результатов исследования. Как показывает опыт ЭАЦ, информация о случившихся инцидентах в тот или иной отчетный период продолжает поступать на протяжении многих месяцев после его завершения.

Стоит отметить, что количество утечек конфиденциальной информации в мире стало резко расти после начала СВО. Во второй половине 2022 года их зарегистрировано в два с лишним раза больше, чем в первой. На Рисунке 1 заметно, что пиковое количество утечек данных случилось в I полугодии 2023 года. Далее начался спад. Посмотрим, насколько эта тенденция окажется продолжительной.

** Количество утечек информации приведено на 15 августа 2024 г. ЭАЦ регулярно обновляет свои базы данных, включает в них новые случаи компрометации данных из коммерческих компаний и госорганизаций в разных странах мира, актуализирует информацию по ранее добавленным инцидентам, связанным с утечками информации, поэтому данные за тот или иной период могут меняться.*

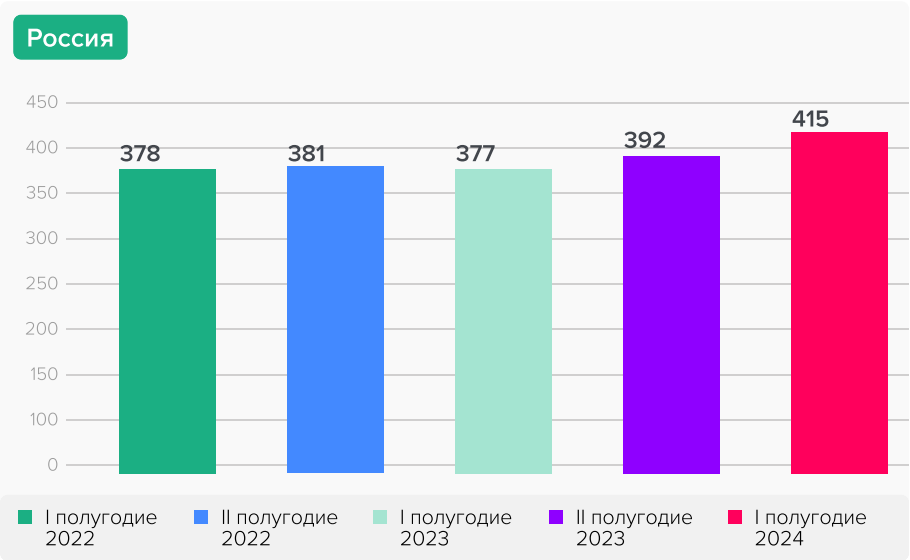
Основной вклад в снижение количества зарегистрированных утечек информации, произошедших в I полугодии 2024 года, внесли Соединенные Штаты Америки. По данным ЭАЦ, инцидентов, связанных с утечками информации, в этом государстве стало меньше на 28,7% (см. Таблицу 1). Однако, отдельные американские коллеги отмечают небольшой рост общего количества нарушений, касающихся компрометации данных (total compromises). По данным ITRC, в I полугодии 2024 года он составил 11,5%. Количество нарушений выросло с 1382 по сумме первых двух кварталов 2023 года до 1541 в первой половине 2024 г. Но общее количество утечек информации в США, зарегистрированных ЭАЦ InfoWatch, все равно больше, поэтому мы продолжаем целиком ориентироваться на собственную методику сбора сведений.

Количество зарегистрированных ЭАЦ утечек информации значительно сократилось и во многих других крупных государствах: Бразилия, Индонезия, Китай, Турция, Япония.

Таблица 1. Количество утечек информации в США, I полугодие 2022 г. - I полугодие 2024 г.

В России, напротив, за рассматриваемый период произошел рост количества утечек информации. Всего в I полугодии 2024 г. зарегистрировано 415 случаев компрометации данных, что на 10,1% больше, чем в I полугодии 2023 г., когда произошло 377 подобных нарушений (Рисунок 2). Такую динамику мы связываем с происходящим вокруг СВО. Вооруженный конфликт имеет тесную связь с противоборством в киберпространстве. С одной стороны, российские компании постоянно подвергаются атакам проукраинских хакерских группировок (прежде всего хактивистов, то есть нарушителей, ставящих целью не получение прибыли, а достижение политических целей, создание медийного эффекта). С другой стороны, российские спецслужбы выявляют на вновь присоединенных территориях и в других регионах РФ нарушителей, которые сливали информацию о войсковых частях и соединениях, вооружении, стратегических объектах и т.д.

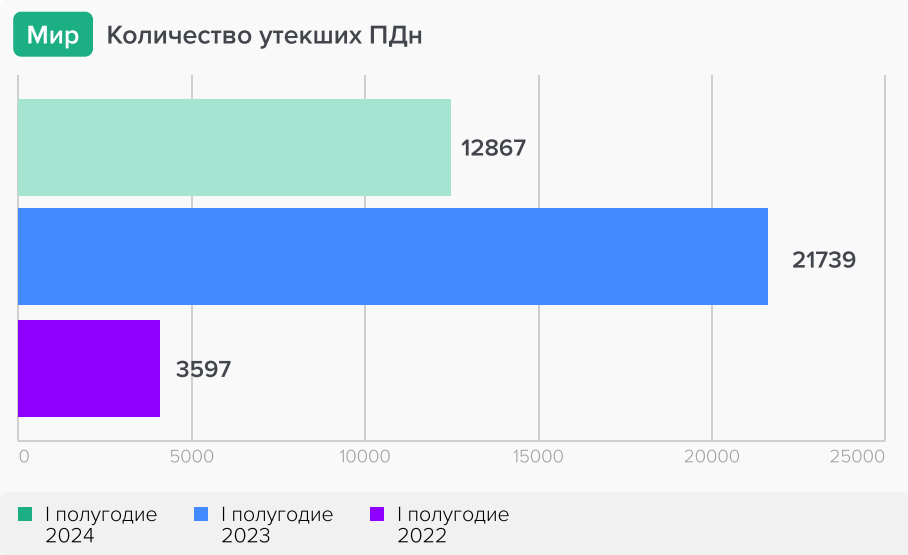
Рисунок 2. Количество утечек информации: Россия, I полугодие 2022 г., I полугодие 2023 г. - I полугодие 2024 г.



В России «утекло» почти миллиард записей персональных данных

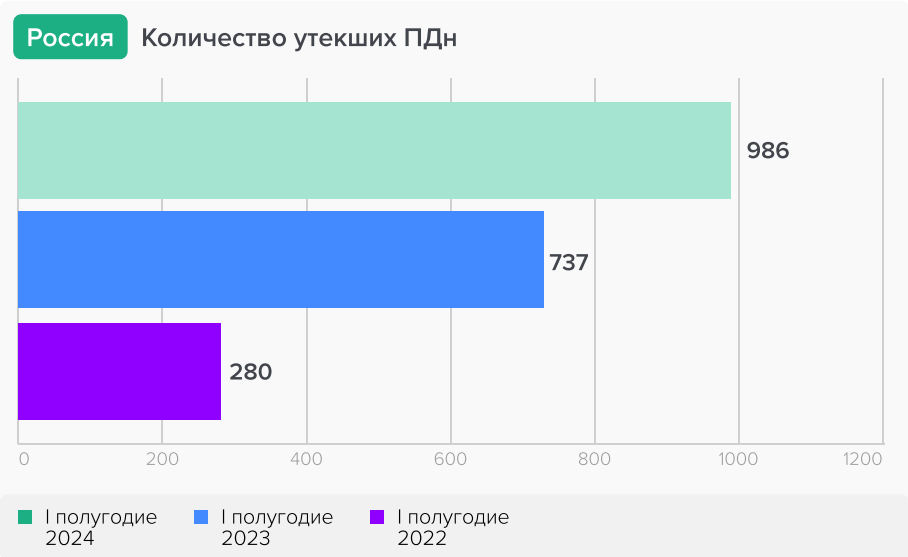
Количество скомпрометированных записей персональных данных в мире по поступившим на данный момент сведениям существенно сократилось. В I полугодии 2024 г. утекло более 12,8 млрд записей, что на 40,8% меньше, чем за аналогичный период прошлого года (Рисунок 3). На фоне общего сокращения количества инцидентов, связанных с утечками данных, стали еще реже утекать крупные базы данных. Если в первой половине 2023 года утекло 577 баз, насчитывающих не менее 1 млн записей ПДн, то в первой половине 2024 года количество таких баз сократилось до 364, то есть более чем на треть (на 36,9%). Количество баз с количеством записей ПДн от 10 млн составило 185 в I полугодии 2023 г. и 119 в I полугодии 2024 г., то есть на 35,7% меньше.

Рисунок 3. Количество утекших записей ПДн (в миллионах): Мир, I полугодие 2022 г., I полугодие 2023 г., I полугодие 2024 г.



В то же время в России отмечен антирекорд по количеству утекших записей персональных данных. Всего за I полугодие 2024 г. скомпрометировано без малого миллиард записей ПДн — 986 млн (Рисунок 4). Это на 33,8% больше, чем в I полугодии 2023 г. *Правда, более половины зарегистрированного в первой половине 2024 года объема утекших данных пришлись на один инцидент, зарегистрированный Роскомнадзором. По данным регулятора в сфере связи, ИТ и массовых коммуникаций, разом были скомпрометированы 500 млн строк данных*.*

Рисунок 4. Количество утекших записей ПДн (в миллионах): Россия, I полугодие 2022 г., I полугодие 2023 г., I полугодие 2024 г.



* *https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3*

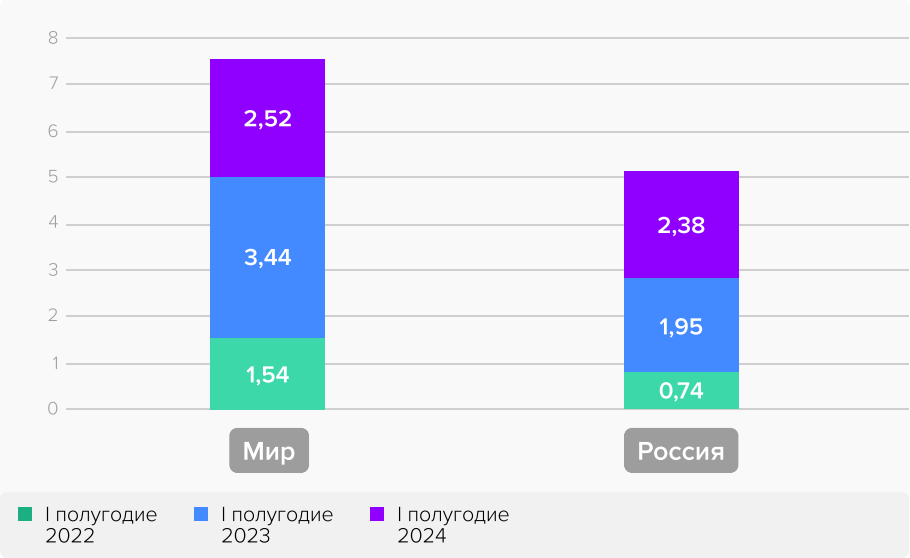
Таким образом, всего за полгода утекло количество единиц персональных данных, которое почти в семь раз превышает население России. Однако, при этом, как и в мире, крупные базы в 2024 году стали утекать реже. По данным ЭАЦ, **количество утекших баз, содержащих не менее 1 млн записей ПДн, в первом полугодии 2023 года составило 56, тогда как в первом полугодии 2024 года их зарегистрировано 31,** то есть на 44,6% меньше.

Баз данных, содержащих 10 млн записей ПДн и более, в первой половине 2023 года в России утекло 14, тогда как за аналогичный период 2024 года их количество составило 9, то есть на 35,7% меньше.

В ходе одного инцидента в среднем утекает 2,52 млн записей ПДн в мире и 2,38 млн записей ПДн в России

Среднее количество записей ПДн в расчете на одну утечку в первых полугодиях 2022- 2024 гг. представлено на Рисунке 5. Интересно, что в первой половине 2024 года в России среднее количество единиц персональной информации составило 2,38 млн записей, практически сравнявшись с мировым показателем (2,52 млн записей). В первых полугодиях 2023 и 2022 годов средняя мировая утечка была примерно вдвое «тяжелее» российской по количеству скомпрометированных записей ПДн.

Рисунок 5. Среднее количество записей персональных данных на одну утечку информации (в миллионах): Мир - Россия, I полугодие 2022 г., I полугодие 2023 г., I полугодие 2024 г.



За I полугодие 2024 года 97,7% всех зарегистрированных утечек информации пришлись на инциденты умышленного характера (Рисунок 6). Доля случайных утечек данных по сравнению с I полугодием 2023 г. незначительно увеличилась - с 2% до 2,3%.

Рисунок 6. Распределение утечек информации по типу умысла: Мир, I полугодие 2023 г. - I полугодие 2024 г.

В России более 99% утечек информации носят умышленный характер

В России доля инцидентов случайного характера сократилась с 1,5% в I полугодии 2023 г. до 0,5% в I полугодии 2024 г. (Рисунок 7). Доминирующая доля умышленных нарушений связана с повышенной активностью внешних нарушителей различных категорий (хакеры, хактивисты, агенты зарубежных спецслужб и т.д.) в ходе СВО, а также с перераспределением инцидентов внутри информационного периметра организаций: в одних случаях такие утечки данных довольно надежно предотвращаются благодаря развитой культуре DLP и других средств защиты, а в других — могут пропускаться из-за относительной слабости систем защиты.

Рисунок 7. Распределение утечек информации по типу умысла: Россия, I полугодие 2023 г. - I полугодие 2024 г.

Мировая доля записей ПДн, скомпрометированных в результате утечек случайного характера, в первой половине 2024 г. составила 2,9% по сравнению с 2,1% за аналогичный период 2023 г. (Рисунок 8). **Самые массовые утечки случайного характера связаны с некорректными настройками облачных хранилищ.** В результате подобных нарушений могут утекать крупные базы

Рисунок 8. Распределение процентов утекших записей ПДн по типу умысла: Мир, I полугодие 2023 г. -I полугодие 2024 г.

В России доля записей персональных данных, скомпрометированных в результате нарушений случайного характера, в I полугодии 2024 года оказалась почти вдвое выше мировой (Рисунок 9)**. Правда, почти все скомпрометированные данные по совокупности таких инцидентов в нашей стране пришлись на один случай:** в феврале 2024 г. исследователи обнаружили утечку 54 млн пользовательских профилей хостинг-провайдера из-за неправильных настроек хранилища на облачной платформе MongoDB*.

** https://cybernews.com/security/web-hosting-ucoz-uid-data-leak/*

Скомпрометированные данные включали адреса электронной почты, номера телефонов, даты рождения, имена пользователей, ID, IP-адреса и временные метки. Кроме того, были раскрыты хэшированные пароли, ответы на секретные вопросы для аутентификации, адреса профилей пользователей в соцсетях, ссылки на фотографии и другие данные. Если к столь большой базе информации доступ успели получить злоумышленники, то они смогут проводить масштабные вредоносные атаки и фишинговые кампании, а также взламывать аккаунты пользователей на разных социальных платформах.

Рисунок 9. Распределение процентов утекших записей ПДн по типу умысла: Россия, I полугодие 2023 г. -I полугодие 2024 г.

В мире и в России выросли доли утечек информации в промышленности и торговле

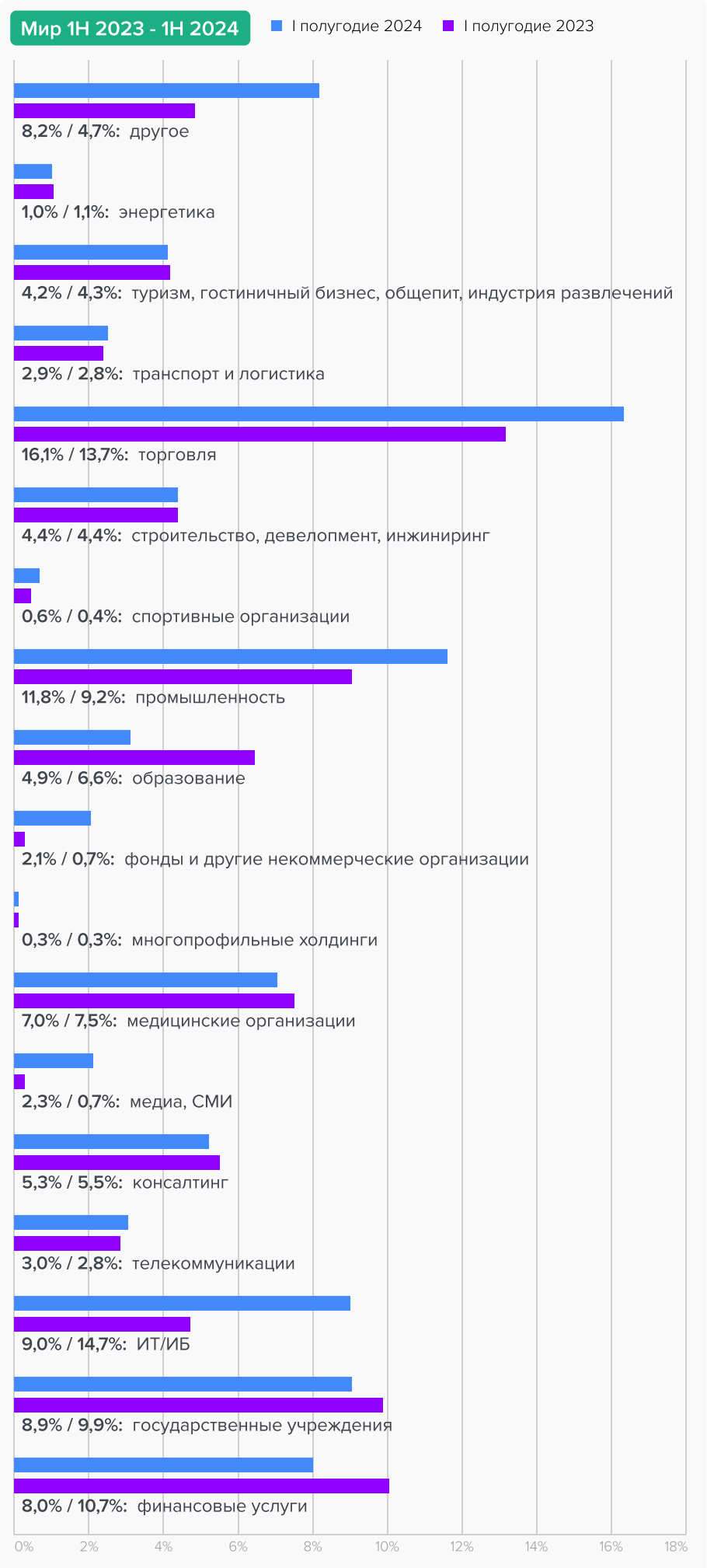
На Рисунке 10 показано отраслевое распределение утечек информации в мире, а на рисунке 11 — в России.

В мире по итогам I полугодия 2024 г. можно выделить увеличение долей торговли (с 13,7% до 16,1%) и промышленности (с 9,2% до 11,8%). Вместе с тем, сократились доли таких отраслей, как финансовые услуги (с 10,7% до 8%), государственные учреждения (с 9,9% до 8,9%), ИТ/ИБ (с 14,7% до 9%), образование (с 6,6% до 4,9%) и ряда других.

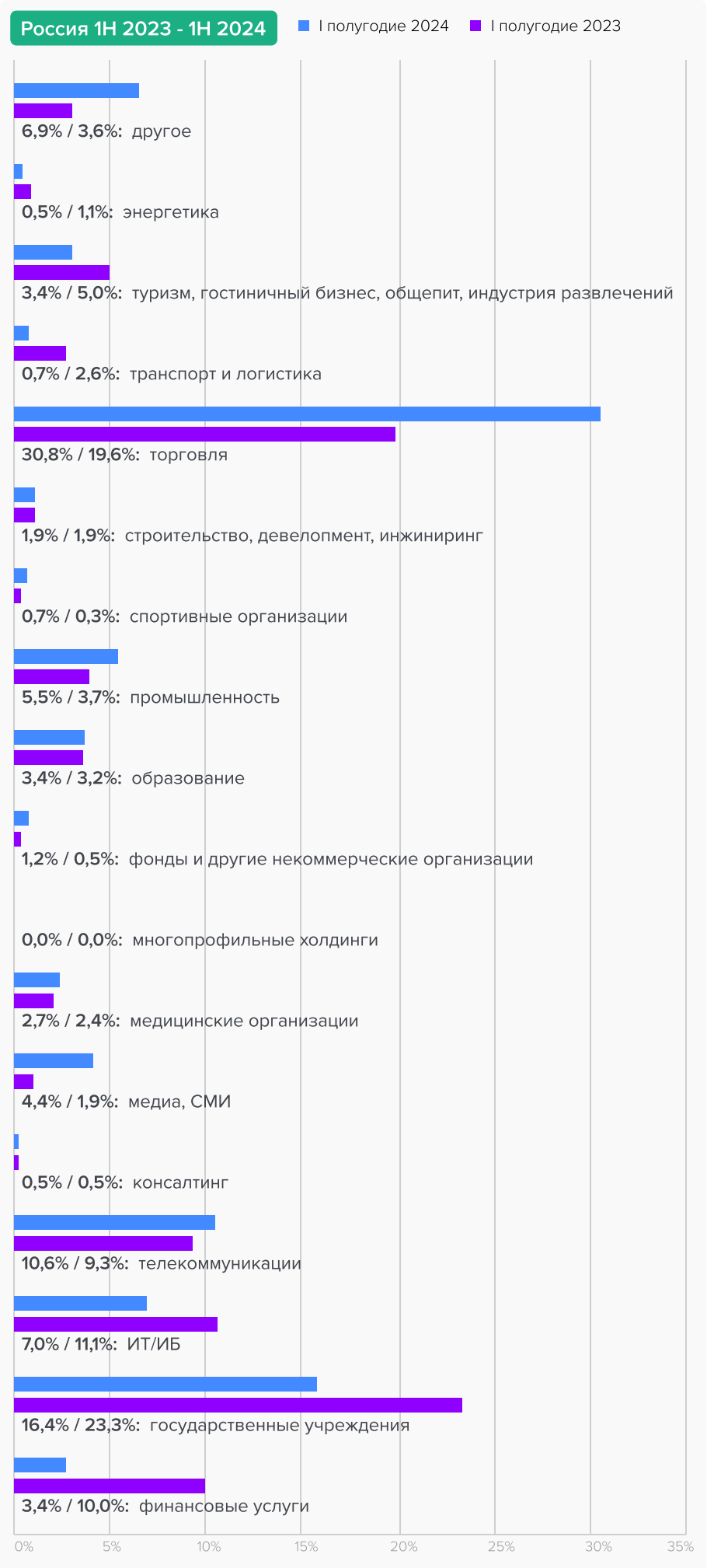
В России наибольшую долю в отраслевом распределении утечек занимает торговля. Если в I полугодии 2023 г. её доля составляла 19,6%, то по итогам I полугодия 2024 г. она выросла до 30,8%. Хакеры постоянно атакуют российские интернет-магазины (в основном небольшие) и других представителей ритейла, пользуясь слабым уровнем информационной безопасности, а то и вовсе ее отсутствием. Именно из-за стремительного роста количества утечек информации в торговле произошёл общий рост количества утечек в России по итогам первого полугодия 2024 года. Также подросла доля промышленности — с 3,7% до 5,5%.

В то же время в российском распределении утечек в первой половине 2024 г. по сравнению с аналогичным периодом 2023 г. снизились доли финансовых компаний (с 10% до 3,4%), государственных учреждений (с 23,3% до 16,4%), ИТ/ИБ (с 11,1% до 7%).

Рисунки 10-11. Распределение утечек информации по отраслям: Мир - Россия, I полугодие 2023 г. - I полугодие 2024 г.



Рисунки 10-11. Распределение утечек информации по отраслям: Мир - Россия, I полугодие 2023 г. - I полугодие 2024 г.



В России наибольший рост утечек отмечен в спортивных организациях, СМИ и НКО. Наибольшее снижение количества утечек произошло в сферах финансов и транспорта

Для представления о динамике изменения количества утечек информации в той или иной отрасли составлена Таблица 2. В ней можно увидеть, что в мире за первое полугодие 2024 г. по сравнению с тем же периодом прошлого года произошел рост количества утечек данных в шести из 18 рассматриваемых отраслевых категорий. Соответственно, в 12 отраслях количество утечек снизилось. В то же время в России случился рост количества утечек в десяти отраслях, а падение зарегистрировано в восьми. **Но делать далеко идущие выводы преждевременно — по итогам года показатели в ряде отраслей могут существенно измениться.**

Таблица 2. Изменение количества утечек информации по отраслям (в %): Мир - Россия, I полугодие 2023 г. - I полугодие 2024 г.

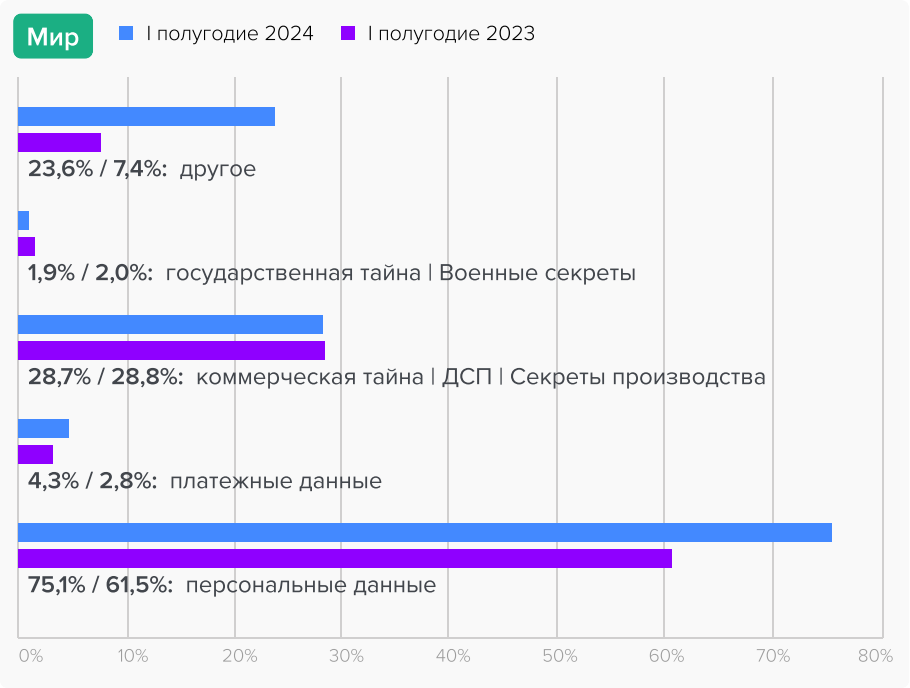
Изменение количества утечек информации в I полугодии 2024 г. по сравнению с I полугодием 2023 г., % (+/-)

Отрасль	Мир	Россия
Финансовые услуги	-40%	-62,2%
Государственные учреждения	-26,8%	-21,8%
ИТ/ИБ	-49,9%	-31%
Телекоммуникации	-14%	+25,7%
Консалтинг	-22,9%	0%
Медиа, СМИ	+155,6%	+157,1%
Медицинские организации	-24,5%	+22,2%
Многопрофильные холдинги	-27,3%	0%
Фонды и другие НКО	+125,5%	+150%
Образование	-40,5%	+16,7%
Промышленность	+3,6%	+64,3%
Спортивные организации	+19,2%	+200%
Строительство, девелопмент, инжиниринг	-18,8%	+14,3%
Государственные учреждения	-26,8%	-21,8%
Торговля	-5,2%	+73%
Транспорт и логистика	-16,2%	-70%
Туризм, гостиничный бизнес, общепит, индустрия развлечений	+20,4%	-26,3%
Энергетика	-24,3	-50%
Другое/Не определено	+44,3%	+107,1%

В мире стали чаще утекать платежные сведения и ПДн, в России — гостайна

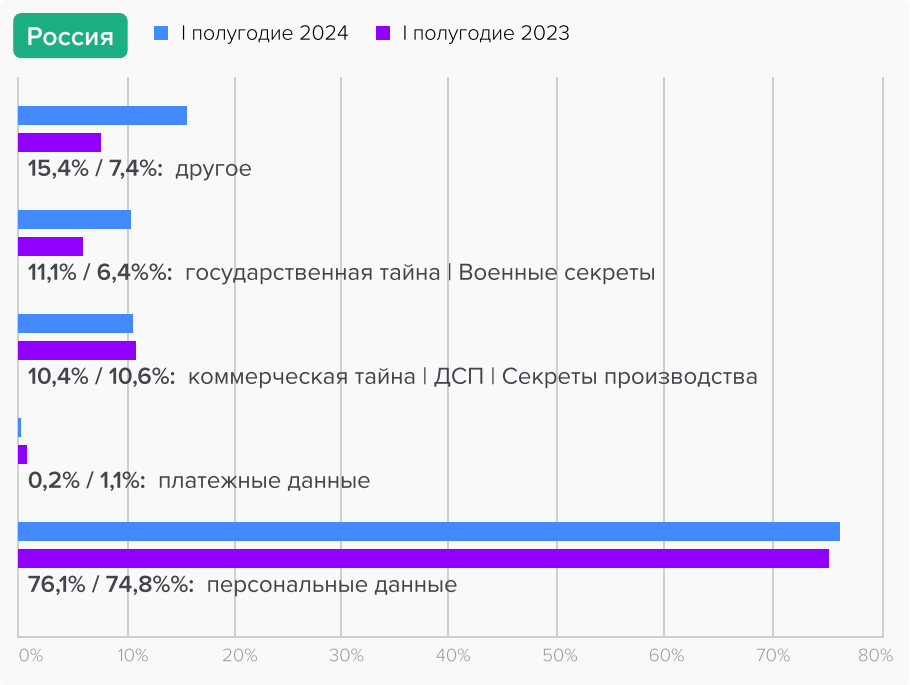
На Рисунках 12-13 приведено распределение утечек информации по типам скомпрометированных данных*.

Рисунок 12. Распределение утечек информации по типам данных: Мир, I полугодие 2023 г. - I полугодие 2024 г.



В России по итогам I полугодия 2024 г. существенно выросла доля государственной тайны (Рисунок 15), что прежде всего связано с регулярным выявлением на фоне СВО лиц, сливающих противнику информацию, связанную с воинскими формированиями и расположением стратегических объектов (по официальным публикациям).

Рисунок 13. Распределение утечек информации по типам данных: Россия, I полугодие 2023 г. - I полугодие 2024 г.



** Сумма долей здесь и в диаграмме на рисунке 15 превышает 100%, так как в ряде случаев утекали несколько типов данных.*

Выявленных утечек по вине сотрудников стало меньше

На Рисунках 14-15 представлено распределение утечек информации в мире и России по виновникам. Можно выделить рост доли внешних нарушителей с одновременным сокращением доли сотрудников.

Рисунок 14. Виновники утечек информации: Мир, I полугодие 2023 г. - I полугодие 2024 г.

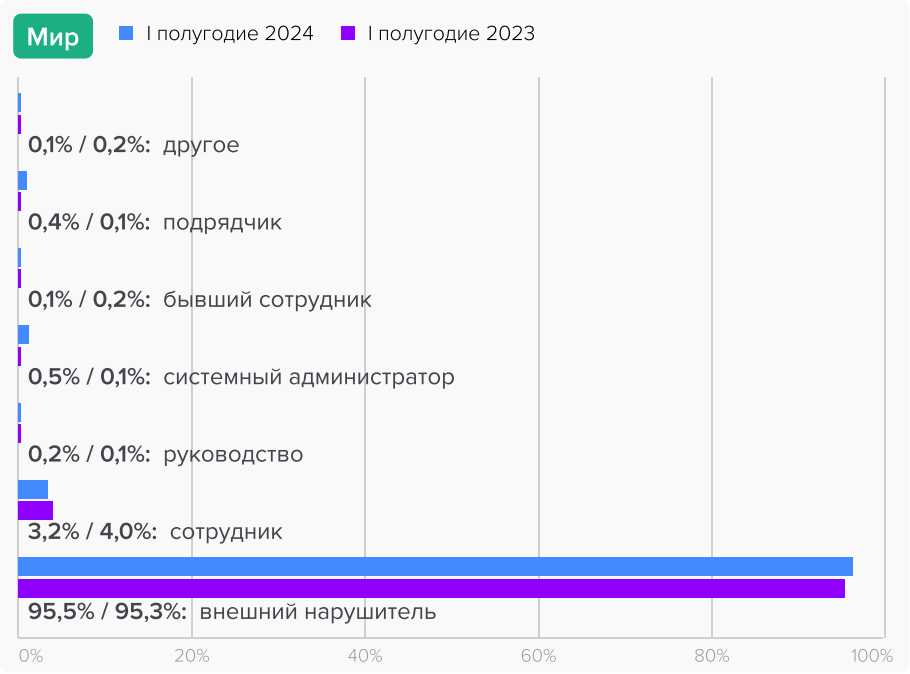


Рисунок 15. Виновники утечек информации: Россия, I полугодие 2023 г. - I полугодие 2024 г.

Важно отметить, что сокращение доли участия (вины) персонала организаций связано с продолжающимися массовыми атаками. Даже если по их итогам хакеры не распространяют украденные данные, это не отменяет факта утечки информации как события, повлекшего утрату контроля над конфиденциальной информации, выхода ее за периметр организации.

В то же время внутренние утечки (по вине персонала компаний) довольно редко становятся известными публике. Такие случаи обычно выносятся в информационное поле в результате возбуждения уголовных дел, судебных разбирательств.

Организации, сотрудник которой допустил утечку данных, как правило, проще скрыть этот факт и разобраться с нарушителем во внесудебном порядке, чем давать объяснения общественности*. Не стоит забывать и про так называемые «гибридные утечки» — нарушения, происходящие в результате сговора внешних злоумышленников и сотрудников.

И хотя формально такие утечки классифицируются как внешние, большую роль в них играет внутренний нарушитель (передача внешним злоумышленникам учетных данных, сведений о ключевых узлах информационной инфраструктуры, ценной информации о руководстве и т.д.).

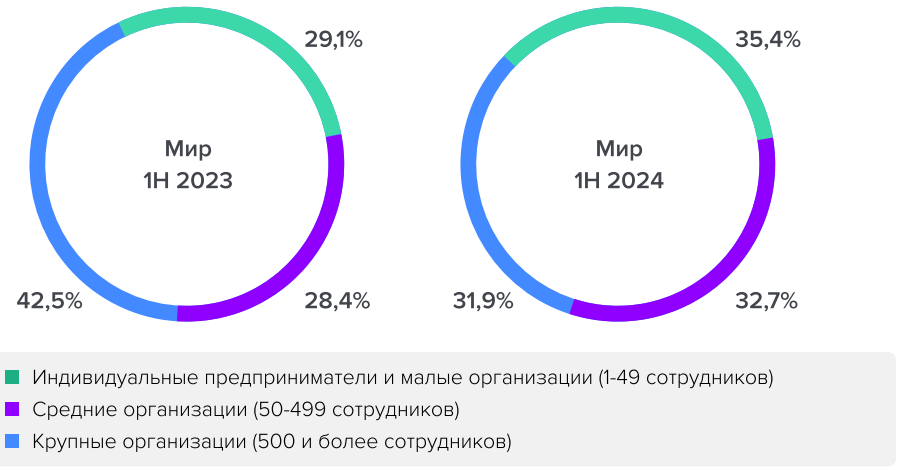
Во всяком случае, на наш взгляд, стоит признать, что культура реагирования на внутренние инциденты в целом по-прежнему остается на уровне «мы не выносим сор из избы». Поэтому доля ставших известными внутренних утечек информации уже много лет остается сравнительно небольшой на фоне интенсивного роста хакерских атак.

В России по итогам I полугодия 2024 г. доля сотрудников в общем распределении виновников утечек данных сократилась до 11,8% (с 18% в I полугодии прошлого года).

В России резко выросла доля утечек среди ИП и малых организаций

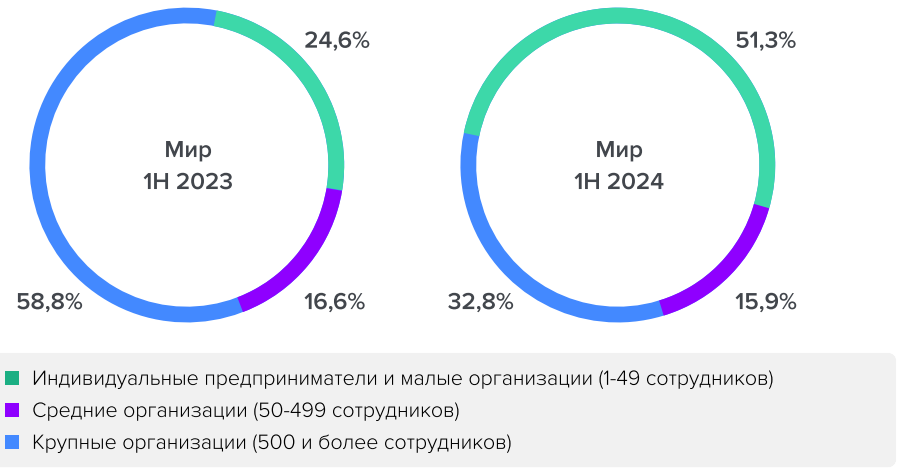
Среди утечек информации в мире с 57,5% до 68,1% выросла общая доля, которую занимают малые и средние организации. Соответственно, на долю крупных организаций (от 500 сотрудников) в I полугодии 2024 г. пришлось менее трети зарегистрированных утечек (Рисунок 16).

Рисунок 16. Распределение пострадавших от утечек организаций по размеру: Мир, I полугодие 2023 г. - I полугодие 2024 г.



В российском распределении организаций, пострадавших от утечек информации, произошли еще более кардинальные изменения (Рисунок 17).

Рисунок 17. Распределение пострадавших от утечек организаций по размеру: Россия, I полугодие 2023 г. - I полугодие 2024 г.



Вдвое — до 51,3% — в первом полугодии 2024 г. выросла доля малых организаций и ИП. Соответственно, резко — с 58,8% до 32,8% — сократилась доля крупных организаций. На основании этих данных можно сделать, что именно малый бизнес в РФ принял основной удар нарушителей в первой половине 2024 года. Речь идет об интернет-магазинах, туристических компаниях, заведениях общепита, небольших СМИ, тематических форумах и ряде других представителей СМБ.

** По данным опросов, в том числе экспертных, в 2023 году.*

Заключение и выводы

Российская картина утечек информации на этот раз имеет существенные отличия от общемировой. Случаев компрометации данных в отечественных организациях за первое полугодие 2024 г. стало примерно на 10% больше по сравнению с аналогичным периодом прошлого года и на 6% больше, чем во втором полугодии 2023 г. Главной причиной увеличения количества утечек данных стал активный накат киберпреступников (прежде всего проукраинских хактивистов) на малый бизнес. От действий злоумышленников особенно часто страдали небольшие торговые организации, многие из которых, скорее всего, не обладают развитыми системами информационной безопасности.

В то же время в мире количество утечек снизилось второе полугодие подряд. Позитивный тренд в основном обеспечен относительными успехами США, где в I полугодии 2024 г. случаев компрометации данных стало меньше почти на 30%, тогда как в мире примерно на 20%. Несмотря на сложную экономическую ситуацию, рынок кибербезопасности в Штатах в последнее время рос более чем на 10% ежегодно. По данным Fortune Business Insights, если в 2022 году объем этого рынка составил 53,59 млрд долларов, то в 2023 году уже 59,27 млрд долларов. Судя по всему, щедрые инвестиции в укрепление защиты информационной инфраструктуры коммерческих компаний и правительственных учреждений позволили более эффективно противостоять волне киберинцидентов. Кроме того, позитивную роль могла сыграть Национальная стратегия кибербезопасности, представленная президентом Байденом в марте 2023 г. Этот основополагающий для США документ по защите цифрового мира сформулировал ключевые принципы ответственности защиты информационной инфраструктуры и стимулировал стратегические планы, а также долгосрочные инвестиции в кибербезопасность. Управление Национального директора по кибербезопасности (ONCD) США методично работает над реализацией 69 инициатив, прописанных в первой итерации плана стратегии.

В I полугодии 2024 года продолжился массовый рост количества атак на организации. Как следствие, растет доля умысла в общем распределении зарегистрированных нарушений. При высокой доле инцидентов, связанных с компрометацией данных в ходе кибератак, в тени находятся внутренние нарушения, то есть инциденты, связанные с действиями персонала. Полагаем, что утечки (и попытки утечек!) по вине персонала зачастую остаются неизвестными общественности, поскольку компаниям не хочется огласки инцидентов. Поэтому чаще всего нарушителей могут просто увольнять, не доводя дело до суда, а если информация не попала в свободный доступ или не стала объектом продажи на форумах, то о ней не узнают или узнают не скоро. Также такие данные могут быть использованы для обогащения других предлагаемых в продажу баз.

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 /infowatchout /infowatch

Методика

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

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.