УДК 004.056 DOI 10.37468/2307-1400-2024-1-46-59

ОСОБЕННОСТИ УТЕЧЕК ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В РОССИЙСКОЙ ФЕДЕРАЦИИ

Гайсина Алина Ринатовна[1]
Филатова Татьяна Александровна[1]
[1] Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург, Россия

АННОТАЦИЯ

Согласно официальным данным за последний год количество утечек персональных данных увеличилось в 4 раза. Количество опубликованных персональных данных в 2023 году превышает общее население Российской Федерации на 50 млн. В исследовании систематизирована статистика утечек информации в разрезе факторов воздействия и по составу утекших данных пользовательской информации в 2022-2023 гг. В ходе анализа статистических данных крупнейших вендоров России определены основные характерные черты утечек персональных данных в 2023 году, выявлены уязвимости отечественного киберпространства. Авторами определены несовершенства законодательного регулирования процессов обеспечения комплексной защиты персональных данных и предложены направления для нивелирования выявленных уязвимостей.

Ключевые слова: персональные данные, утечки информации, киберинцидент, мошенники, информационная инфраструктура, кибератака, цифровой портрет, внешний нарушитель, гибридная атака, политический фактор, компрометация.

FEATURES OF RESTRICTED ACCESS INFORMATION LEAKS IN THE RUSSIAN FEDERATION

Gaysina Alina R.[1]
Filatova Tatyana A.[1]
[1] St. Petersburg State University of Economics, St. Petersburg, Russia

ABSTRACT

According to official data, over the past year the number of personal data leaks has increased 4 times. The number of published personal data in 2023 exceeds the total population of the Russian Federation by 50 million. The study systematizes the statistics of information leaks in the context of impact factors and the composition of leaked user information in 2022-2023. In the course of analyzing statistical data from the largest vendors in Russia, the main characteristic features of personal data leaks in 2023 were identified and the vulnerabilities of domestic cyberspace were identified. The author identified the imperfections of legislative regulation of the processes of ensuring comprehensive protection of personal data and proposed directions for leveling the identified vulnerabilities.

Keywords: personal data, information leaks, cyber incident, fraudsters, information infrastructure, cyber attack, digital portrait, external intruder, hybrid attack, political factor, compromise.

Введение

В России на конец 2023 года нет единого информационно-статистического инструментария, позволяющего объективно оценивать количество киберинцидентов[1] в разрезе ключевых характеристик: по характеру, по объему ущерба, по периоду реализации. Доступные для анализа данные чаще относятся к узким отраслям функционирования хозяйствующих субъектов, группам частных лиц со специфичными характеристиками, обслуживаемым через конкретный центр мониторинга информационной безопасности (Security operation center)[2] [1].

Данный фактор формирует сложности в процессе выявления прямой зависимости между ростом количества атак и количеством утечек. Несмотря на это, комплексная оценка имеющихся статистических данных позволяет сформировать основные тренды в действиях преступных лиц, нацеленность мошеннических группировок на определенные сегменты киберпространства и предупредить ущерб от потенциальных атак [2].

1 Событие информационной безопасности, влекущее потенциальные риски несанкционированного доступа к информации с целью её дальнейшей эксплуатации, модификации и нарушения целостности работы IT-систем.

2 Структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов.

Аналитическая часть

Согласно имеющимся данным экспертно-аналитического центра InfoWatch, более 80% утечек в 2023 году в России были спровоцированы кибератаками. При этом в последние два года количество утечек по вине внешнего нарушителя увеличилось почти в 6 раз (см. рисунок 1) [3].

С одной стороны, данный факт является положительной оценкой применения методов борьбы с внутренним нарушителем: приведение комплексной системы противодействия внешним атакам организации в соответствии с актуальными угрозами, повсеместное применение эффективных инструментов защиты потоков информации (DLP-системы, борьбу с нелояльными сотрудниками и др.) [5]. Так, общее количество утечек в результате внутреннего воздействия составило на конец 2023 года – 76 случаев, что ниже уровня 2022 года на 45% [3].

Однако, следует учитывать и то, что развитие информационного киберпространства при высоких темпах развития информационных технологий способствует появлению новых форм преступлений, повышая латентность внутренних утечек информации (см. рисунок 2).

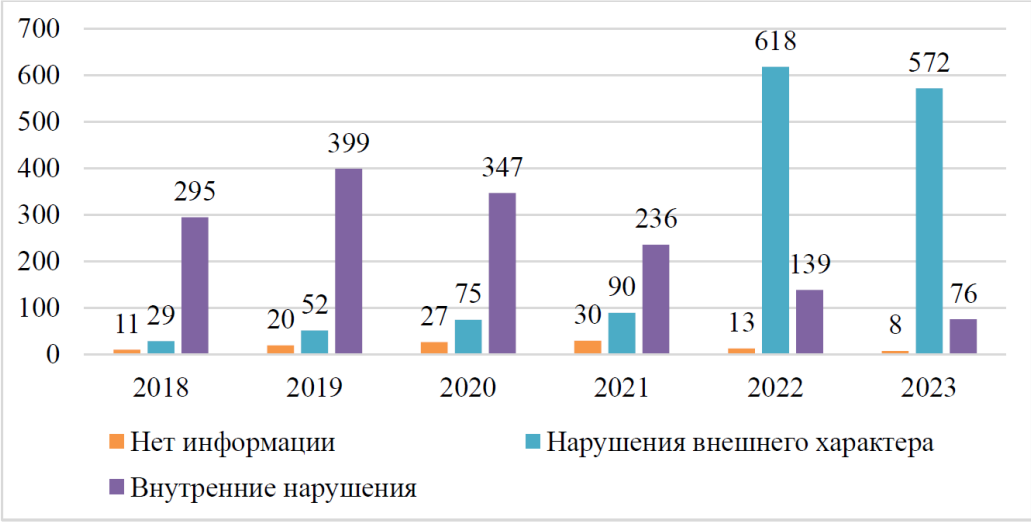

Рисунок 1 – Динамика утечек по характеру воздействия в динамике 2018-2023 гг., шт.

Источник: составлено автором на основе [3, 4]

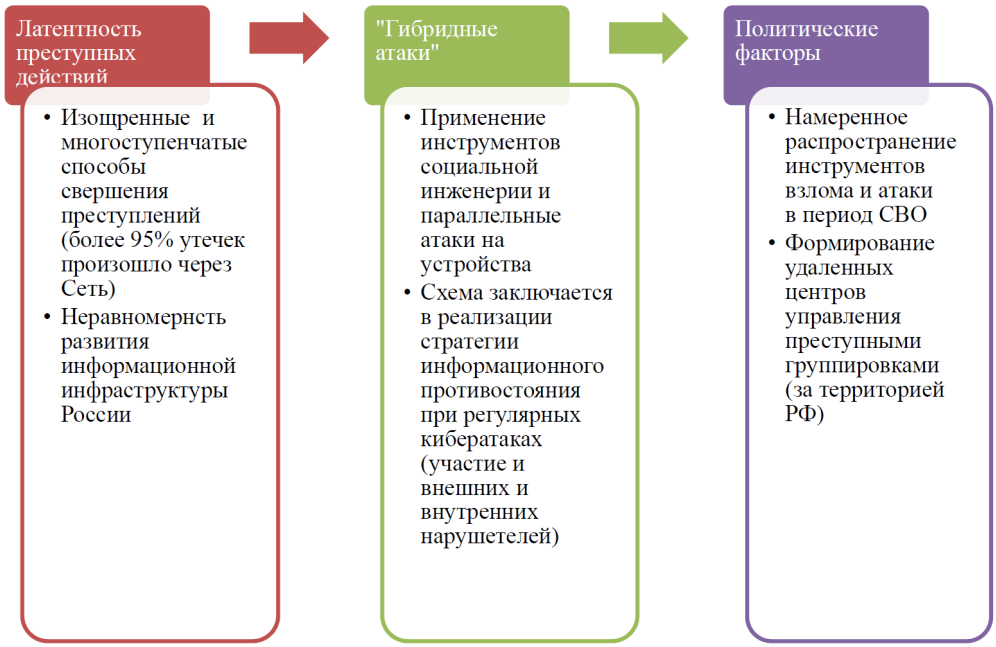

Рисунок 2 – Факторы развития киберпреступности в 2022-2023 гг.

Источник: составлено автором

В том числе, нельзя отрицать эффективность использования мошенниками комбинированных инструментов свершения атак: полученные из внутреннего информационного пространства субъекта ликвидные данные систематизируются и модифицируются для дальнейшей эксплуатации и компроментации. Большинство кибератак скорее являются отвлекающим маневром мошенников в процессе нанесения ущерба информационной инфраструктуре субъектов России. Таким образом, угроза утечки информации становится все более неопределенной во времени и месте реализации, что в условиях современных политико-экономических условий становится одним из главных факторов угроз национальной безопасности [5].

Рост запросов на владение информацией, составляющей государственную тайну, способствовал снижению доли утекших персональных данных в 2023 году до 80,3% (см. рисунок 3). Частота возбуждения уголовных дел по обвинению в шпионаже и госизмене по данным картотеки российских судов стала регулярной (начиная с марта 2023 года[3]).

Тем не менее, персональные данные остаются главным видом утекших данных. За последний год в общем количестве было украдено около 100 баз данных, что на 28% больше, чем в 2022 году. При этом мотивы преступников претерпели трансформацию: в 2022-2023 гг. значительно вырос запрос на хактивизм[4], большое количество таких атак было совершено проукраинскими группировками с целью дестабилизации инфраструктуры России.

В подтверждение развития гибридных атак, прослеживается четкая схема выведения из строя всех элементов критической инфраструктуры России (см. рисунок 4): намечен параллельный стремительный рост украденных данных в малых организациях России (в сравнении с 2022 годом

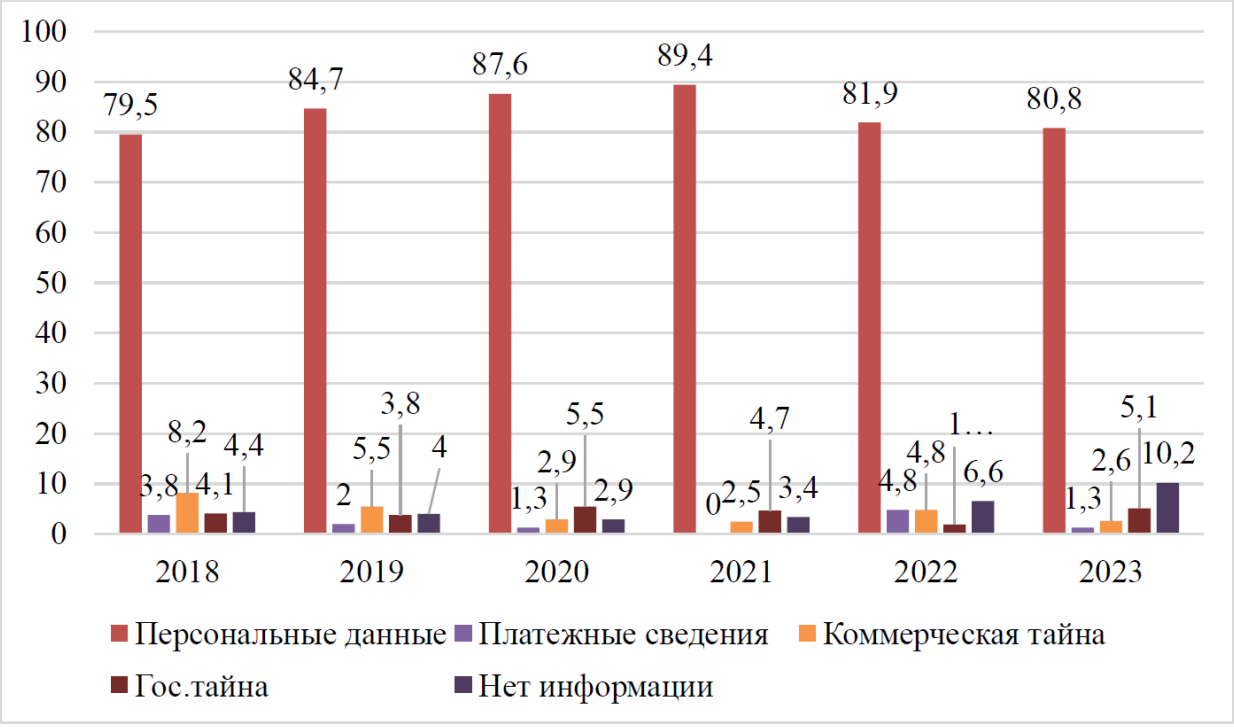

Рисунок 3 – Распределение типов информации при утечках в динамике 2018-2023 гг., %

Источник: составлено автором на основе [3, 4, 6]

3 С 1 января по 31 июля 2023 года в России возбудили не менее 90 уголовных дел о госизмене (статья 275 УК РФ), шпионаже (статья 276 УК РФ) и сотрудничестве на конфиденциальной основе (статья 275.1 УК РФ). По данным Kaspersky Digital Footprint Intelligence суды рассмотрели 87 протоколов Роскомнадзора, составленных по факту утечек данных, и назначили штрафы на сумму больше 4,6 млн руб. При этом сравнительно низкая доля «утекшей гос.тайны» обусловлена высокой степенью засекреченности рассматриваемых разбирательств.

4 Форма цифрового активизма, нелегальные способы использования информационных средств (устройств, сетей) с целью продвижения политических, социальных и иных идей.

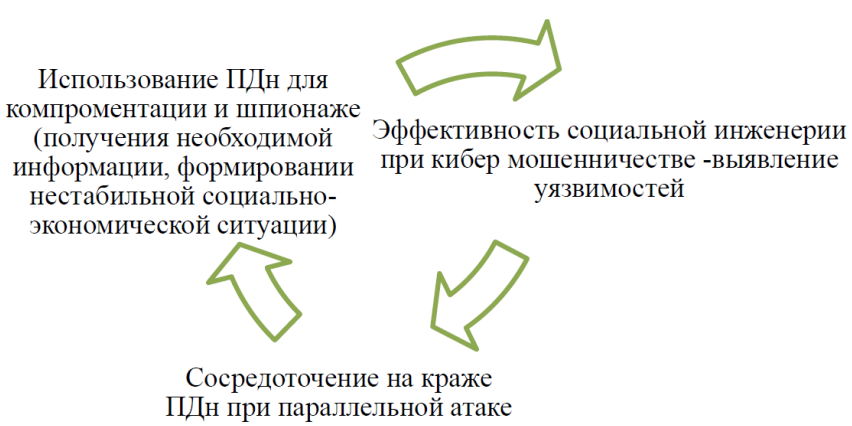

Рисунок 4 – Причинно-следственная связь прямого и косвенного воздействия на элементы критической инфраструктуры России

Источник: составлено автором на основе [1, 4, 10]

(18,5%) в 2023 году процент вырос до 34,1%) [7]. Совокупная успешность хакерских атак стала гораздо выше: на 1 утечку в 2023 году в среднем приходится 1709 тыс. записей ПДн, тогда как в 2022 году – 912 тыс. записей (см. рисунок 5) [8]. Средняя стоимость одной записи утекших данных в зависимости от канала получения и вида запрошенной информации в нелегальных сетях варьируется от 20 до 700 долларов [9].

Опасность представляет также и тот факт, что мошенники оперируют вариативными базами персональных данных (государственные сервисы, социальные сети, торговые маркетплейсы, страховые компании, учреждения здравоохранения и др.), последовательно дополняя и расширяя цифровой портрет гражданина РФ[5] [1]. Последствия от утечек «цифровой личности» в узком смысле увеличивают финансовые риски мошенничества

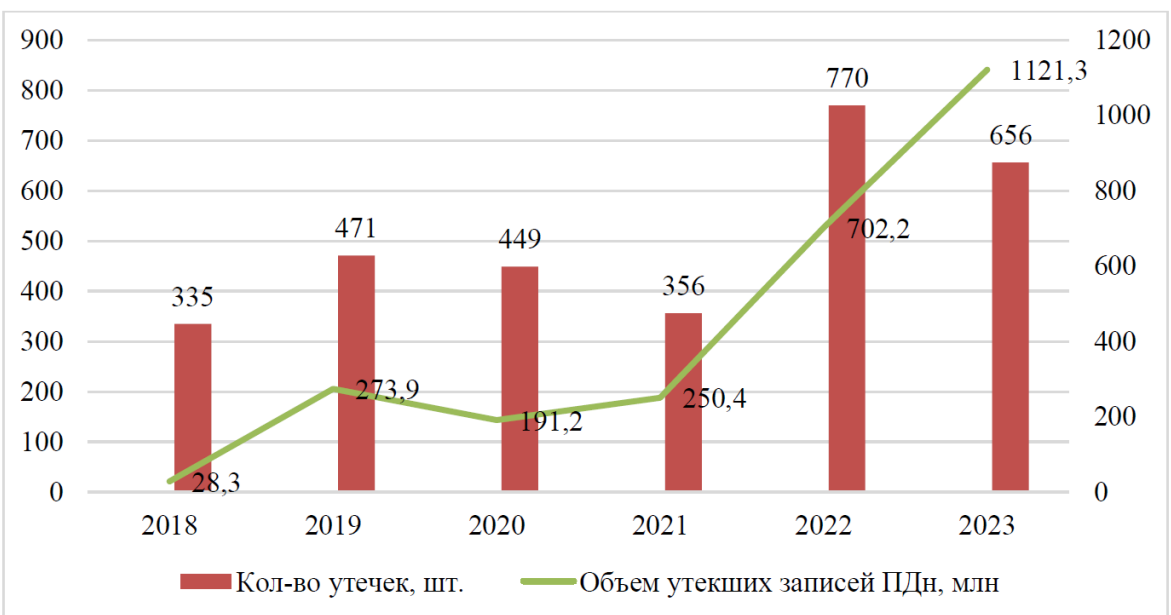

Рисунок 5 – Динамика утекших персональных данных (ПДн) в динамике 2018-2023, тыс. шт.

Источник: составлено автором на основе [4, 11]

5 Цифровой портрет гражданина РФ – систематизация всех данных гражданина, которые имеются в электронных базах и государственных информационных системах.

и нарушения конфиденциальности личной жизни гражданина, в широком смысле – становятся инструментом шантажа – мощным оружием в экономических и политических конфликтах, которые рассматриваются некоторыми группами мошенников неотъемлемой частью политического противостояния [4].

В ответ на регулярные вызовы 4 декабря 2023 года в Государственной Думе Российской Федерации в первом чтении был принят проект об увеличении оборотных штрафов за утечки персональных данных. В зависимости от объема ущерба за утечку данных должностным лицам грозит штраф на сумму до 2 млн рублей, юридическим – до 15 млн. Одновременно вводится уголовная ответственность за использование, передачу, сбор и хранение персональных данных, полученных незаконным путем, а также за создание информационных ресурсов, распространяющих такие данные (с максимальным сроком лишения свободы до 10 лет) [12].

По мнению представителей отраслевых ассоциаций увеличение оборотных штрафов не является эффективной мерой в борьбе с утечкой ПДн граждан ввиду того, что критерии разграничения вины (причастности) хозяйствующего субъекта и внешнего нарушителя в непосредственном преступлении размыты и неясны [12].

В действительности, динамика роста штрафов в последние три года свидетельствует о существенном увеличении нагрузки на российский бизнес, которая вынуждает увеличивать расходы на обеспечение информационной безопасности (см. рисунок 6).

У большинства компаний МСП недостаточно финансовых ресурсов для адаптации информационных систем безопасности, тогда как с увеличением оборотных штрафов ситуация существенно ухудшится. Согласно данным «Лаборатории Касперского», общий рынок кибербезопасности в прогнозируемом сценарии на ближайшие полтора года будет увеличен на 18-20%, что в фактическом объеме составляет более 250 млрд рублей инвестиций [6]. Соответственно, в условиях трансформации отечественного киберпространства и сопровождающихся процессах импортозамещения увеличение оборотных штрафов влечет критические риски для IT-отрасли.

Нецелесообразность формирования государственного инструмента регулирования состава правонарушения (утечки) также проявляется в порядке определения суммы оборотного штрафа

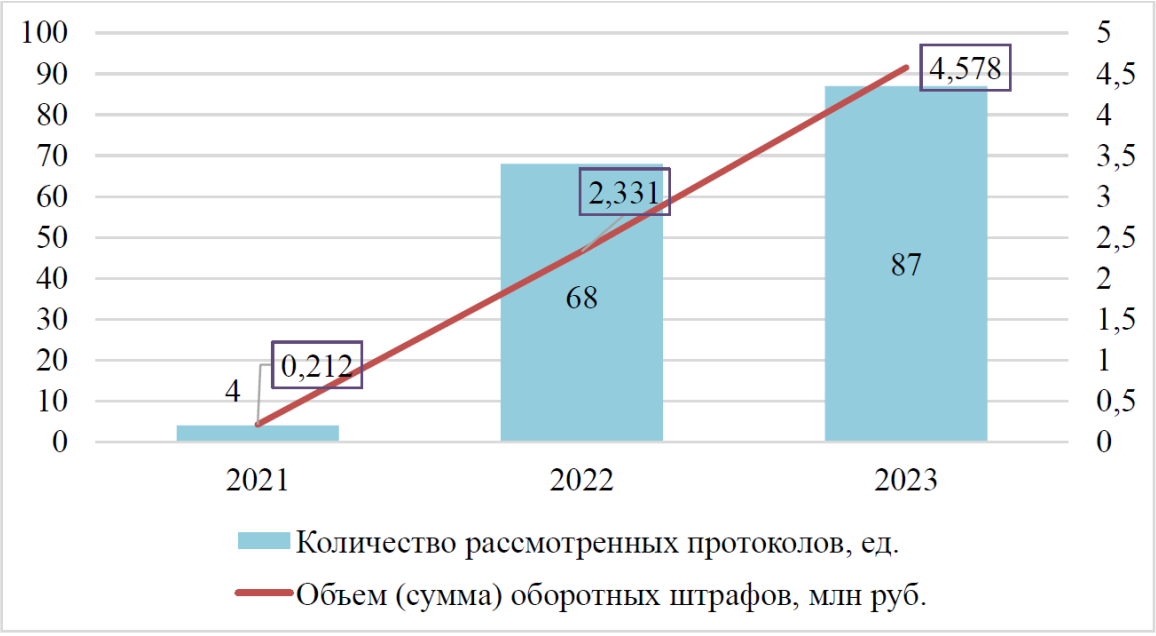

Рисунок 6 – Динамка увеличения оборотных штрафов за утечки персональных данных, 2021-2023 гг.

Источник: составлено автором на основе [2, 13]

в общей сумме выручки компании -нарушителя порядка обработки персональных данных. Такой непропорциональный рост дополнительных затрат компаний при высокой инфляции может противоречиво отразиться и на конечном потребителе (покупателе), что в перспективе полностью нейтрализует положительные превентивные меры государственной поддержки.

По словам начальника отдела информационной безопасности компании SearchInform, в ситуации с увеличением оборотных штрафов реакция бизнеса может трансформироваться из активной позиции в пассивную: при отсутствии учета фактора невиновности и беспричастности к утечке персональных данных компании могут байкотировать интеграцию защитных мер информационной безопасности [13].

Так, при повторном инциденте утечки персональных данных размер штрафа для компании будет составлять 0,1-0,3% от выручки в пределах от 15 до 500 млн рублей. При этом порядок реализации положений не соответствует принципам справедливости и пропорциональности административной ответственности: по мере увеличения выручки компании доля штрафа сокращается – см. рисунок 7. (размер оборотного штрафа для компаний может отличаться более чем в 60 раз) [12, 14].

За отсутствием общего регламента к проведению внутреннего расследования – непредоставление информации о свершившимся инциденте и его причинах в Роскомнадзор влечет возникновение отягчающих обстоятельств для оператора. При этом сроки проведения внутреннего расследования оператора до сообщения об утечке ПДн (24 часа) не учитывают специфику современных преступлений: как правило, мошенники могут оперировать старыми базами данных, эксплуатировать уязвимости компаний-партнеров [15].

На фоне рассмотрения на законодательном уровне предложений по увеличению оборотных штрафов представители Ассоциации больших данных (АБД)[6] в ноябре 2023 года разработали отраслевой стандарт по защите данных. Данный документ был предложен в качестве альтернативы поправкам как категориальный алгоритм оценки эффективности внутренних механизмом обеспечения безопасности персональных данных [5]. Главная концепция отраслевого регламента заключается в возможности компаний самостоятельно

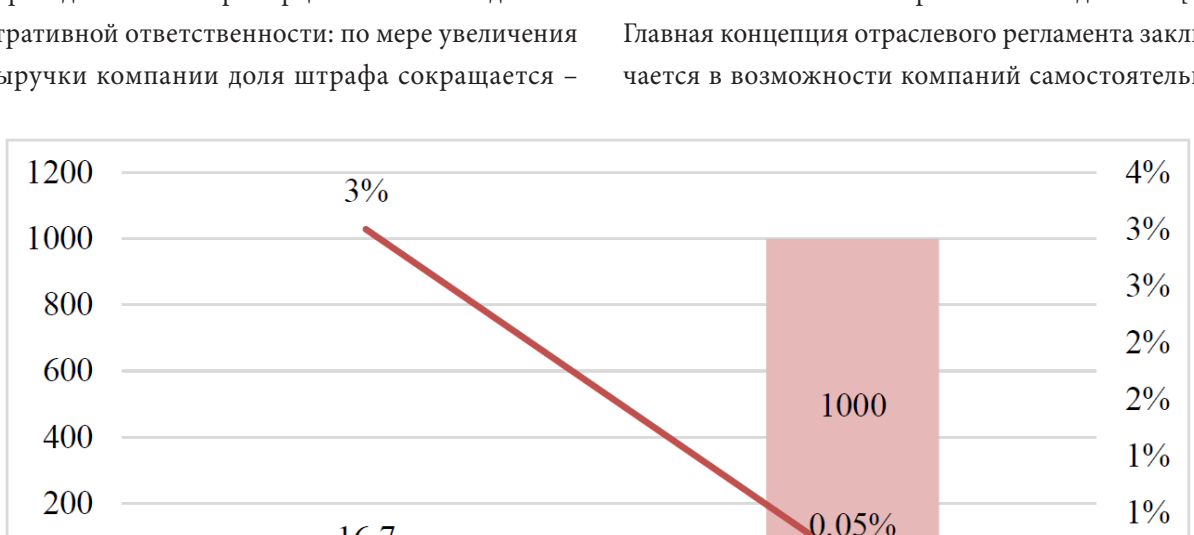

Рисунок 7 – Непропорциональность административной ответственности

Источник: составлено автором на основе [13, 14]

6 Ассоциация больших данных – саморегулируемое объединение крупных игроков отечественного IT-рынка, среди которых «Яндекс», Сбербанк, «Мегафон», «Ростелеком», VK и др. Главными приоритетами объединения является выработка адаптивных условий для развития технологий и технологических решений для движения больших данных.

оценивать безопасность киберинфраструктуры данных и привлекать сторонних экспертов для независимой экспертизы, обязуя ответственных участников разрабатывать планы-контрасты для минимизации выявленных уязвимостей и дальнейшей валидации необходимого уровня защиты персональных данных. В то время как наложение оборотных штрафов накладывает двойные расходы на компанию при любом исходе (согласно исследованию Positive Technologies доказать невиновность компании при утечке ПДн возможно лишь в 0,8% случаев [11]), отраслевой стандарт определяет дифференциальный подход к ущербу, что, как следствие, может быть применено при расчете оборотного штрафа[7].

Вопреки многочисленным обращениям со стороны бизнеса с просьбой учесть смягчающим обстоятельством крупные инвестиционные вложения в кибербезопасность – поправки в первом чтении приняты в первоначальной форме. Категоричная позиция органов власти строится на приоритезации положений ФЗ-152, который регулирует отношения в сфере обработки персональных данных. Тем не менее члены Ассоциации на конференции Data Fusion в апреле 2024 года подписали отраслевой регламент, что в очередной раз подтверждает нацеленность бизнеса на принятие эффективных превентивных мер по защите информационный безопасности [5].

С одной стороны, можно согласиться с мнением о том, что стандарт АБД выступает дополнительной мерой поддержки и защиты, позволяя участникам IT-рынка внедрять лучшие практики для принятия эффективных и необходимых мер защиты. Однако данный стандарт не освобождает операторов ПДн от рисков наложения штрафов в случае утечки ввиду того, что причастность и умышленность действий нарушителя определяет Роскомнадзор, основываясь на положениях закона.

Более того, категоризация ущерба в положениях отраслевого стандарта и поправках не является идентичной, что также формирует сложности в процессе формирования доказательственной базы невиновности оператора ПДн в случае его непричастности в утечке персональных данных [5, 16].

Данная ситуация характеризует отсутствие однонаправленности и согласованности в действиях государства и бизнеса в процессе формирования безопасности инфраструктуры страны. Согласно докладу Центра стратегических разработок одной из основных угроз информационной безопасности России является отсутствие институциональной среды для практического применения инструментов защиты информации [3].

Безусловно, нормативно-правовая защита персональных данных граждан РФ не ограничена санкционными мерами: в период 2022-2023 гг. государство активно мотивировало бизнес наращивать уровень надежности систем информационной безопасности в сфере использования персональных данных [2, 9]. С 1 марта 2023 года действуют усилительные контрольные меры: трансграничная передача данных через получение согласия Роскомнадзор[8]; регламентация процессов уничтожения персональных данных; запрет на автоматическую обработку биометрических данных и др. [12].

Однако на практике многие внутренние регламентирующие документы о порядке обработки, использования и уничтожения персональных данных организаций являются формализованными и не адаптированы под особенности конкретного бизнеса и потребности клиентов. На конец 2023 года по данным компании «Б-152» политики конфиденциальности 55% банков не соответствуют требованиям 152-ФЗ в части указания конкретных целей обработки персональных данных[9] [8].

7 Данный подход применяется и в рамках Общих правил защиты данных, используемом в мировой практике (GDPR -General Data Protection Regulation).

8 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

9 В исследовании специалистов компании «Б-152» проводилось подробное изучение политик конфиденциальности более 300 отечественных банков (с универсальной и базовой лицензией).

Во многом это обусловлено отсутствием методических материалов и рекомендаций по адаптации внутренних IT-инфраструктур под требования законодательства. К тому же, высокая волатильность и трансформация информационного пространства требует применения лучших практик, тогда как нормативно-правовая среда ограничена во времени. В мире существуют примеры положительной интеграции государственного регулирования (в качестве базового направления и минимально необходимого условия функционирования) и деятельности отраслевого сообщества (в качестве конкретизации требований по обеспечению безопасности защиты ПДн, алгоритма принятия оперативных мер по выявлению инцидентов нарушения в сфере их использования)[10].

Согласно положениям ФЗ-152, для того чтобы обрабатывать персональные данные сотрудником ответственной организации не предусмотрено получение определенного уровня квалификации[11] [15]. Ввиду того, что каждая организация, которая собирает и обрабатывает персональные данные является оператором ПДн, целесообразно установить требования к специалисту (по уровню лояльности и квалификации).

Отсутствие понимания ответственного за обработку ПДн сотрудника о возможной утечке информации влечет риски халатности, как следствие, увеличение финансовых рисков для компании (особенно в условиях увеличения оборотных штрафов). Например, в США и Китае институт сферы персональных данных закрепляет обязанность оператора ПДн проводить системное обучение сотрудников, допущенных к обработке персональных данных (см. таблица 1).

Более того, в Китае крупным компаниям – базовым интернет-провайдерам (в России – компании, предоставляющие услуги сопровождения телекоммуникационной сети), необходимо создавать независимые надзорные органы, в состав которых входят внешние сотрудники – представители экспертного сообщества. Данные контрольно-надзорные органы наряду

Таблица 1 – Сравнительный анализ регулирования института обработки персональных данных в США, России и Китае [10, 17]

Критерий	США	Россия	Китай
Нормативно-правовая база регулирования	Общегосударственные законы, законы штатов.	ФЗ-152, предписания ФСБ и ФСТЭК России.	Personal Information Protection Law.
Мелодические материалы	Национальный институт стандартов и технологий (NIST)	ФСБ, ФСТЭК России.	Министерство промышленности и информационных технологий (MIIT), Министерство общественной безопасности и Государственная администрация по регулированию рынка.
Обязательное обучение сотрудников организации	Обязует проводить системное обучение сотрудников базовым и специальным знаниям в сфере обработки ПДн.	Отсутствует требования к сотрудникам.	Обязует проводить обучение сотрудника по защите данных аналогично положениям DPO в GDPR.
Порядок разработки политик/ стандартов обработки персональных данных компаний	Отдельное специальное руководство № SP 800-122, содержащее порядок применения организационных, технических и юридических мер (трактование требований регулятора к обеспечению безопасности обработки персональных данных).	ФЗ-152, предписания ФСБ и ФСТЭК России.	Администрация киберпространства КНР, Технический комитет по стандартизации НИБ.

10 В США, Великобритании, Китае наряду с нормативными актами компании активно используют дополнительные стандарты. В финансовом секторе России также есть положительный опыт: наряду с требованиями регулятора ЦБ, деятельность участников рынка должна также соответствовать требованиям стандарта PCI DSS.

11 Организация (оператор ПДн) обязан назначить ответственное лицо, которое буде отвечать за обработку персональных данных сотрудников, клиентов и других граждан (ч. 1 ст. 22.1). При этом сотрудник подотчетен непосредственному руководителю.

с сотрудниками должны быть сертифицированы и лицензированы на должность ответственных за контроль соблюдения правил защиты данных (аналогично DPO в GDPR) [17]. Несмотря на применение радикальных методов концепции Zero Trust[12] в отношении безопасности данных граждан в Китае, использование общих принципов «нулевого доверия» (необходимость подтверждения прав доступа, общий принцип «незащищенности данных») в отношении обеспечения безопасности персональных данных может принести положительные результаты [10].

В то же время отличительной особенностью США от России в сфере обработки персональных данных является и обязанность операторов в создании гибкой политики управления персональными данными, которая должна включать подробный перечень требований к сотруднику при осуществлении своих обязанностей, требования к реагированию на входящие вызовы и потенциальные угрозы нарушения, порядок получения и ограничения прав доступа к персональным данным. Грамотная адаптация под особенности странового развития США идеи «нулевого доверия» в процессе обработки персональных данных заключается в требованиях законодателя минимизировать персональные данные и использовать методы шифрования, которые существенно затрудняют незаконную идентификацию личности [17, 18].

Примечательно, что несмотря на активный рост утечек ПДн в мире в 2023 году, доля утекших персональных данных гораздо ниже, чем в России (см. рисунок 8).

К тому же наращивание «стоимости» одной утечки для мира в целом положительно в динамике: в 2023 году «стоимость» одной утечки в мире снизилась на 0,3 млн записей, тогда как в России выросла почти в 2 раза (см. рисунок 9) [19].

Используя положительный опыт зарубежных стран, возможна адаптация рекомендаций по обязанности оператора ПДн организовывать и использовать в работе инструменты системного обучения сотрудников в сфере обработки персональных данных. К тому же, согласно опросу InfoWatch среди наиболее эффективных мер в процессе обеспечения информационной безопасности участники отечественного

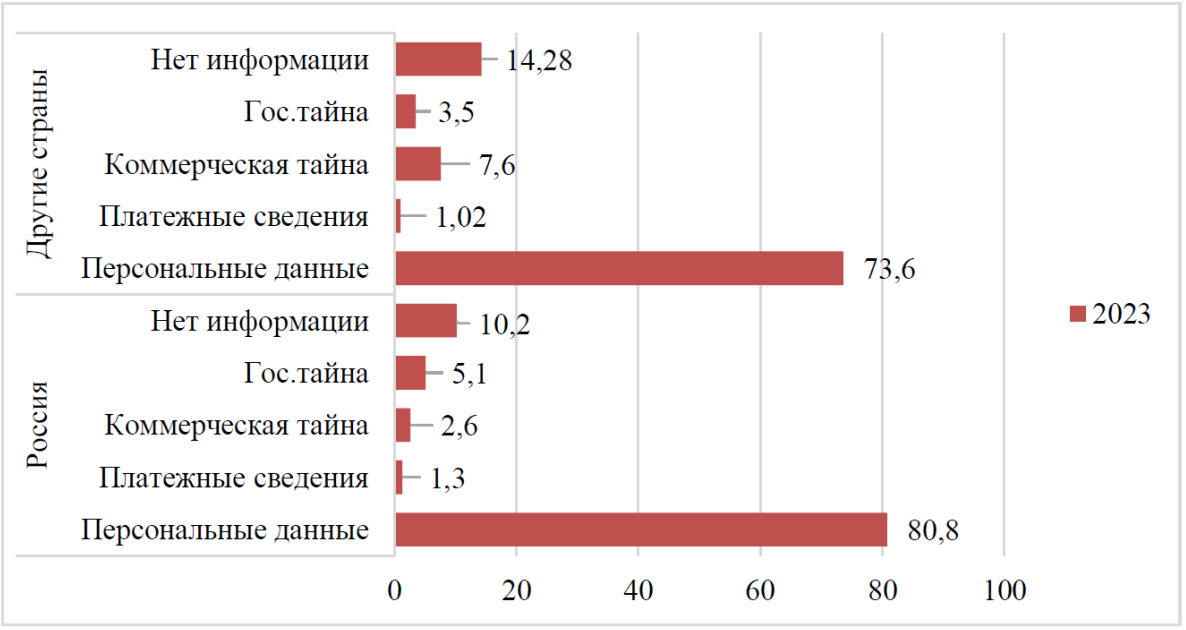

Рисунок 8 – Структура утекших данных в России и мире, 2023 г.

Источник: составлено автором на основе [11, 19]

12 Концепция нулевого доверия – в Китая реализуется на принципах «социального доверия» в соответствии со страновым менталитетом.

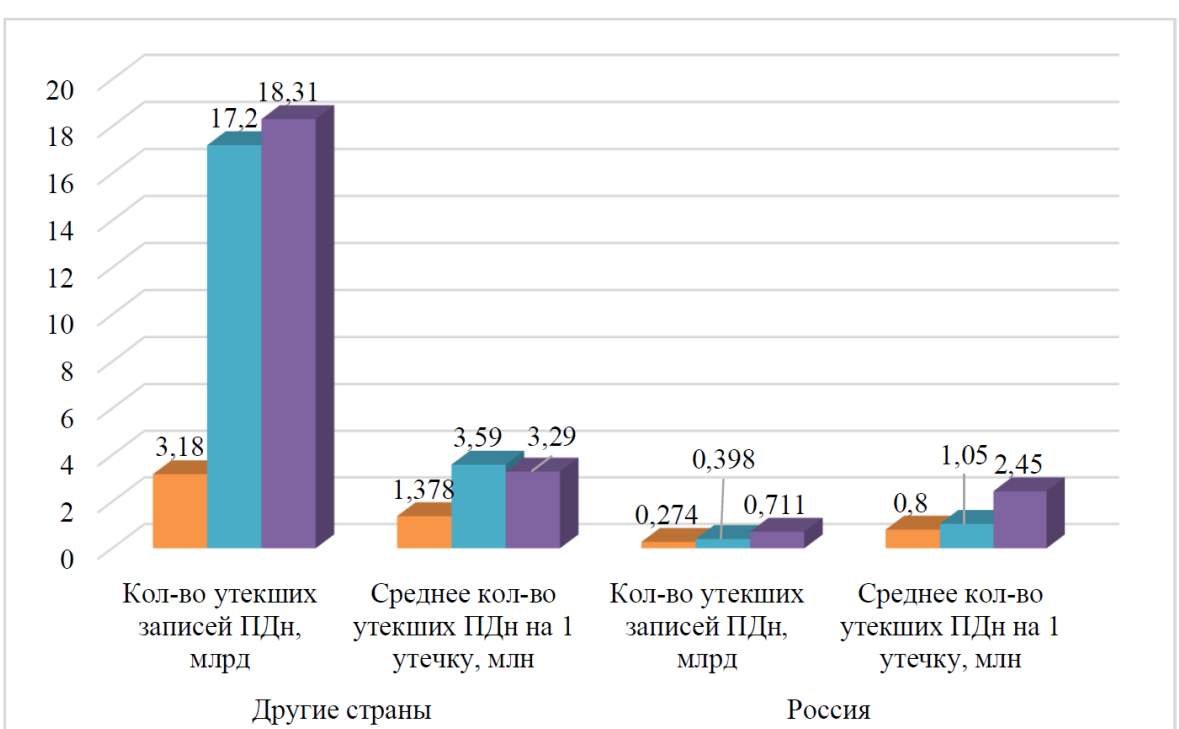

Рисунок 9 – Количество утекших данных и количество утекших строк ПДн на 1 утечку в России и мире, 2022-2023 гг.

Источник: составлено автором на основе [6, 20, 21]

рынка называли организацию обучающих мероприятий и внедрение элементов кибергигиены в рабочие процессы (более 55% респондентов) [3].

Заключение

Наиболее вероятно, что качественной предупредительной мерой в процессе формирования контрольной системы обеспечения безопасности персональных данных в правовой среде может стать лицензирование сотрудников, допущенных к обработке персональных данных, по результатам прохождения адаптированной программы обучения (подготовки).

Основными критериями лицензирования должны стать аспекты идентификации сотрудников массивов информации, которые являются персональными данными; понимание действующих требований к обеспечению защиты персональных данных; порядок предоставления и ограничения доступа к ПДн; действия, необходимые для нейтрализации выявленных нарушений и при возникновении угроз обработки ПДН. Учитывая прогнозируемый стремительный рост рынка Security Awareness[13] к 2027 году до 2,35млрд руб. (в 2023 году более 600 млн руб.), обеспечение актуализации элементов системного обучения работы с ПДн не представит труда для отечественных операторов [20].

Таким образом, наращивание правовой экспертизы в процессе реализации деятельности операторов ПДн потребует адаптации формализованных политик конфиденциальности субъектов, разработки специфичной методологии порядка работы с персональными данными. Данный процесс с одной стороны, повысит прозрачность условий обработки персональных данных для граждан, в то же время – сформирует четкие границы ответственности оператора ПДн в процессе осуществления своих полномочий (доказательственная база для суда и отстаивания прав на рынке – см. рисунок 10).

13 Сегмент IT-рынка, предоставляющий решения для повышения уровня киберграмотности сотрудников.

Рисунок 10 – Нейтрализация пробелом институциональной среды кибепространства России в процессе перехода из развивающейся инфраструктуры в развитую

Источник: составлено автором

В то же время, в общей институциональной системе киберинфраструктуры России рассмотрение инициатив отраслевых ассоциаций и учет дифференциального механизма определения уровня ущерба – как следствие, штрафа, за утечку ПДн способствует снижению рисков избыточной криминализации и снизит нагрузку на участников рынка, позволив укреплять внутреннюю систему обеспечения информационной безопасности.

Список литературы

1. *Панин О.Н., Сулейменова Р.Д.* Угрозы безопасности цифрового профиля гражданина РФ // Молодой ученый. – 2022. – № 16 (411). – С. 34-35. – EDN MUIMBO.

2. Департамент информационной безопасности Центрального Банка России: аналитические материалы о противодействии мошенническим практикам в 2023 году. [Электронный ресурс]. – Режим доступа: https://cbr.ru/information_security/pmp/ (дата обращения: 04.09.2023).

3. Экспертно-аналитический центр InfoWatch: Россия: утечки информации ограниченного доступа, 2022-2023 годы. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (дата обращения: 07.02.2024).

4. *Филатова Т.А., Гайсина А.Р., Назаров П.В.* Направления противодействия преступлениям с использованием компьютерных технологий в Российской Федерации // Kant. – 2023. – № 4(49). – С. 166-174. – DOI 10.24923/2222-243X.2023-49.31. – EDN KIJLQY.

5. Российский провайдер сервисов по защите информационной безопасности ГК «Солар»: «Утечки персональных данных: где можно найти чувствительную информацию о сотрудниках и клиентах компании». [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/services/jsoc/blog/3772/?ysclid=luprn0tbtm771806862 (дата обращения: 07.02.2024).

6. Kaspersky Digital Footprint Intelligence: «О значимых утечках данных в России в 2023 году». [Электронный ресурс]. – Режим доступа: https://dfi.kaspersky.ru/data-leakage-2023?reseller=kl-ru_dfi-web_leg_enterprise_oth___b2b_press-release_lnk_____&utm_campaign=dfi-web&utm_source=press-release&utm_

medium=other&utm_term=textlink (дата обращения: 07.02.2024).

7. Экспертно-аналитический центр InfoWatch: отчет о новых проектах в области биометрических персональных данных. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/novye-proekty-v-oblasti-biometricheskikh-personalnykh-dannykh (дата обращения: 03.09.2023).

8. FBK Cybersecurity: «Ужесточение санкций за утечки ПДн». [Электронный ресурс]. – Режим доступа: https://fbkcs.ru/ujestochenie-shtrafnikh-sankciy-za-utechki-pdn (дата обращения: 07.02.2024).

9. Банк России: инциденты информационной безопасности (итоги 1 квартала 2023 года). [Электронный ресурс]. – Режим доступа: https://cbr.ru/press/event/?id=15814 (дата обращения: 03.09.2023).

10. *Власенко В.Э.* Кибератаки: как государства реагируют на инциденты, затрагивающие кибербезопасность информационных систем на современном этапе международного информационного права // Молодой ученый. – 2021. – № 48 (390). – С. 208-211. – EDN PQGCCK.

11. Positive Technologies: отчет «Кибербезопасность. Тренды 2022-2023 годов». [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (дата обращения: 01.09.2023).

12. Российская газета: «Об увеличении оборотных штрафов за утечки персональных данных клиентов». [Электронный ресурс]. – Режим доступа: https://rg.ru/2023/08/28/ostaviat-v-tajne.html?ysclid=luprrog3uv954853994 (дата обращения: 07.02.2024).

13. SearchInform Risk and compliance management: утечка персональных данных и последствия. [Электронный ресурс]. – Режим доступа: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/utechki-personalnyh-dannyh/posledstviya/?ysclid=lup5autaa0598945573 (дата обращения: 07.02.2024).

14. WebsiteRating: 50 тенденций кибербезопасности на 2023 год. [Электронный ресурс]. – Режим доступа: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/ (дата обращения: 03.09.2023).

15. О персональных данных: Федерального закона от 27.07.2006 № 152. [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=luprjoevw3874488925 (дата обращения: 07.02.2023).

16. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор): судебная практика за 2023 год. [Электронный ресурс]. – Режим доступа: https://new.rkn.gov.ru/activity/jurisprudence/p1268/ (дата обращения: 07.02.2024).

17. Российская газета: позиции России и Китая по вопросам кибербезопасности во многом совпали. [Электронный ресурс]. – Режим доступа: https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html?ysclid=lmf70b5s99932142437 (дата обращения: 28.08.2023).

18. *Агаев Р.Ш., Агаев Р.Ш., Графов А.А.* Безопасность информационного сопровождения в системе экономической безопасности // Национальная безопасность и стратегическое планирование. – 2022. – № 2(38). – С. 98-104. – DOI 10.37468/2307-1400-2022-2-98-104. – EDN JLFFQV.

19. RTM Group: мошенничество в сети (судебная практика и ключевые аспекты). [Электронный ресурс]. – Режим доступа: https://rtmtech.ru/research/online-fraud-research/?ysclid=lmepdfenp1273256146 (дата обращения: 28.08.2023).

20. Positive Technologies: «Исследование целевых атак на российский бизнес в 2023 году». [Электронный ресурс]. – Режим доступа: https://vc.ru/flood/317584-informaciya-reputaciya-dengi-politika-pochemu-hakery-atakuyut-rossiyskie-kompanii (дата обращения: 07.02.2024).

21. *Варзин С.А., Матвеев В.В.* Обеспечение информационной безопасности в системе здравоохранения // Национальная безопасность и стратегическое планирование. – 2023. – № 3(43). – С. 19-56. – DOI 10.37468/2307-1400-2024-2023-3-19-56. – EDN ONKEFE.

References

1. *Panin O.N., Suleimenova R.D.* Threats to the security of the digital profile of a citizen of the Russian Federation // Young scientist. – 2022. – No. 16 (411). – pp. 34-35. – EDN MUIMBO.

2. Information Security Department of the Central Bank of Russia: analytical materials on combating fraudulent practices in 2023. [Electronic resource]. – Access mode: https://cbr.ru/information_security/pmp/ (access date: 09/04/2023).

3. Expert and analytical center InfoWatch: Russia: leaks of restricted access information, 2022-2023. [Electronic resource]. – Access mode: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (access date: 02/07/2024).

4. *Filatova T.A., Gaisina A.R., Nazarov P.V.* Directions for combating crimes using computer technologies in the Russian Federation // Kant. – 2023. – No. 4(49). – pp. 166-174. – DOI 10.24923/2222-243X.2023-49.31. – EDN KIJLQY.

5. Russian provider of information security protection services, GC Solar: "Personal data leaks: where you can find sensitive information about the company's employees and clients." [Electronic resource]. – Access mode: https://rt-solar.ru/services/jsoc/blog/3772/?ysclid=luprn0tbtm771806862 (access date: 02/07/2024).

6. Kaspersky Digital Footprint Intelligence: "On significant data leaks in Russia in 2023." [Electronic resource]. – Access mode: https://dfi.kaspersky.ru/data-leakage-2023?reseller=kl-ru_dfi-web_leg_enterprise_oth___b2b_press-release_lnk_______&utm_campaign=dfi-web&utm_source=press-release&utm_medium=other&utm_term=textlink (access date: 02/07/2024).

7. Expert-analytical center InfoWatch: report on new projects in the field of biometric personal data. [Electronic resource]. – Access mode: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/novye-proekty-v-oblasti-biometricheskikh-personalnykh-dannykh (access date: 09/03/2023).

8. FBK Cybersecurity: "Tightening sanctions for personal data leaks." [Electronic resource]. – Access mode: https://fbkcs.ru/ujestochenie-shtrafnikh-sankciy-za-utechki-pdn (access date: 02/07/2024).

9. Bank of Russia: information security incidents (results of the 1st quarter of 2023). [Electronic resource]. – Access mode: https://cbr.ru/press/event/?id=15814 (access date: 09/03/2023).

10. *Vlasenko V.E.* Cyber attacks: how states react to incidents affecting the cybersecurity of information systems at the present stage of international information law // Young scientist. – 2021. – No. 48 (390). – pp. 208-211. – EDN PQGCCK.

11. Positive Technologies: report "Cybersecurity. Trends for 2022-2023." [Electronic resource]. – Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (access date: 09/01/2023).

12. Russian newspaper: "On increasing turnover fines for leaks of personal data of clients." [Electronic resource]. – Access mode: https://rg.ru/2023/08/28/ostaviat-v-tajne.html?ysclid=luprrog3uv954853994 (access date: 02/07/2024).

13. SearchInform Risk and compliance management: leak of personal data and consequences. [Electronic resource]. – Access mode: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/utechki-personalnyh-dannyh/posledstviya/?ysclid=lup5autaa0598945573 (date of access: 02/07/2024).

14. WebsiteRating: 50 cybersecurity trends for 2023. [Electronic resource]. – Access mode: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/ (access date: 09/03/2023).

15. On personal data: Federal Law of July 27, 2006 No. 152. [Electronic resource]. – Access mode: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=luprjoevw3874488925 (date of access: 02/07/2023).

16. Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor): judicial practice for 2023. [Electronic resource]. – Access mode: https://new.rkn.gov.ru/activity/jurisprudence/p1268/ (access date: 02/07/2024).

17. Rossiyskaya Gazeta: the positions of Russia and China on cybersecurity issues largely

coincided. [Electronic resource]. – Access mode: https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html?ysclid=lmf70b5s99932142437 (access date: 08/28/2023).

18. *Agaev R.Sh., Agaev R.Sh., Grafov A.A.* Security of information support in the economic security system // National security and strategic planning. – 2022. – No. 2(38). – pp. 98-104. – DOI 10.37468/2307-1400-2022-2-98-104. – EDN JLFFQV.

19. RTM Group: online fraud (judicial practice and key aspects). [Electronic resource]. – Access mode: https://rtmtech.ru/research/online-fraud-research/?ysclid=lmepdfenp1273256146 (date of access: 08/28/2023).

20. Positive Technologies: "Research of targeted attacks on Russian business in 2023." [Electronic resource]. – Access mode: https://vc.ru/flood/317584-informaciya-reputaciya-dengi-politika-pochemu-hakery-atakuyut-rossiyskie-kompanii (date of access: 02/07/2024).

21. *Varzin S.A., Matveev V.V.* Ensuring information security in the healthcare system // National security and strategic planning. – 2023. – No. 3(43). – P. 19-56. – DOI 10.37468/2307-1400-2024-2023-3-19-56. – EDN ONKEFE.

Статья поступила в редакцию 10 февраля 2024 г.
Принята к публикации 25 марта 2024 г.

Ссылка для цитирования: Гайсина А.Р. Филатова Т.А. Особенности утечек информации ограниченного доступа в Российской Федерации // Национальная безопасность и стратегическое планирование. 2024. № 1(45). С. 46-59. DOI: https://doi.org/10.37468/2307-1400-2024-1-46-59

For citation: Gaysina A.R., Filatova T.A. Features of restricted access information leaks in the Russian Federation // National security and strategic planning. 2024. № 1(45). pp. 46-59. DOI: https://doi.org/10.37468/2307-1400-2024-1-46-59

Сведения об авторах:

ГАЙСИНА АЛИНА РИНАТОВНА – *Факультет бизнеса, таможенного дела и экономической безопасности, Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург, Россия*
ORCID: https://orcid.org/0009-0003-8375-5969
SPIN-код: 5503-7149
e-mail: alinagaysina020401@gmail.com

ФИЛАТОВА ТАТЬЯНА АЛЕКСАНДРОВНА – *доктор экономических наук, доцент, профессор кафедры экономической безопасности, Факультет бизнеса, таможенного дела и экономической безопасности, Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург, Россия*
SPIN-код: 3670-5718
e-mail: werck@rambler.ru

Information about authors:

GAYSINA ALINA R. – *Faculty of Business, Customs and Economic Security, St. Petersburg State Economic University, St. Petersburg, Russian Federation*
ORCID: https://orcid.org/0009-0003-8375-5969
SPIN-код: 5503-7149
e-mail: alinagaysina020401@gmail.com

FILATOVA TATYANA A. – *Doctor of Economic Sciences, Associate Professor, Professor of the Department of Economic Security, Faculty of Business, Customs and Economic Security, St. Petersburg State Economic University, St. Petersburg, Russian Federation*
SPIN-код: 3670-5718
e-mail: werck@rambler.ru