В. В. Зиновьева,
аспирант,
Российский университет транспорта

АНАЛИЗ ИНЦИДЕНТОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РОССИИ И МИРЕ В I ПОЛУГОДИИ 2022 ГОДА. ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. Предмет исследования – правовые проблемы информационной безопасности в России. Цель – разработка и апробация способов решения выявленных правовых проблем по защите информации конфиденциального характера, включая персональные данные. Гипотеза исследования предполагает, что безопасность информации в значительной степени зависит от мировых и внутригосударственных экономических и политических событий. Применены следующие методы: формально-юридический, сравнительно-правовой анализ, диагностический анализ. Выявлена закономерность связи утечки данных с внешнеполитическими и внутриэкономическими процессами. Выводы: действующее российское законодательство в области информационной безопасности нуждается в унификации, выработке нового, отвечающего современным реалиям понятийного аппарата, а также в детализации и конкретизации существующих терминов и определений. Области применения результатов: в теоретической сфере для повышения степени защиты конфиденциальной информации на законодательном уровне, в практической деятельности при обработке персональных данных и привлечения к ответственности за нарушения в области обработки персональных данных.

Ключевые слова: право, цифровые технологии, информационная безопасность, нарушение безопасности конфиденциальной информации, утечка данных, инцидент, персональные данные, неправомерный доступ, передача персональных данных

ANALYSIS OF CONFIDENTIAL INFORMATION BREACH IN RUSSIA AND IN THE WORLD IN THE 1H 2022. LEGAL PROBLEMS OF INFORMATION SECURITY AND SOLUTIONS

Annotation. The subject of the research is the legal problems of information security in Russia. The goal is to develop and test methods for solving identified legal problems related to the protection of confidential information, including personal data. The research hypothesis suggests that information security is highly dependent on global and domestic economic and political developments. The following methods were applied: formally legal, comparative legal analysis, diagnostic analysis. The regularity of the connection between data leakage and foreign policy and domestic economic processes is revealed. Conclusions: the current Russian legislation in the field of information security needs to be unified, to develop a new conceptual apparatus that meets modern realities, as well as to detail and specify existing terms and definitions. Areas of application of the results: in the theoretical realm, to improve realm of the protection of confidential information at the legislative level, in practical activities in

the processing of personal data and holding accountable for violations in the field of personal data processing.

Keywords: Law, Digital technologies, Information security, Confidential information breach, Data leakage, Incident, Personal data, Unauthorized access, Transfer of personal data

Стремительное развитие технологий, инновационные процессы, научные открытия оказывают огромное влияние на развитие общества. Характерной чертой указанных процессов является неуклонное наращивание производства и распространения информации. В современных реалиях ценность информации быстро повышается, что неизбежно ведет к увеличению различных угроз преступных и несанкционированных посягательств на информационную безопасность. Наиболее актуальной проблемой в информационном мире является нарушение безопасности информации ограниченного доступа. Повышенный спрос на обладание конфиденциальными сведениями и данными порождает рост предложений предоставления неправомерного доступа к ним на черном рынке. Под нарушением безопасности конфиденциальной информации (confidential information breach) понимается нарушение безопасности, приводящее к случайному или противозаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к конфиденциальной информации [9]. Такое понятие официально используется в странах ЕС, но в России, к сожалению, не применяется. Однако во внутренних нормативно-правовых актах встречаются следующие формулировки: «утечка информации конфиденциального характера» [4], «утечка информации ограниченного доступа и персональных данных» [2]. Такой понятийный аппарат не отражает в полной мере все многообразие неправомерных действий, которым может подвергаться безопасность конфиденциальной информации. Например, в отношении персональных данных законодатель предлагает оперировать такой формулировкой, как «факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных» [3]. При этом Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных в России – на своем официальном сайте использует термин «утечки ПД» в разделе «инциденты» [5]. Автор полагает, что понятие «утечки ПД» и понятие «инциденты», во-первых, нетождественны, а во-вторых, должны использоваться в рамках более емкого и универсального понятия – «нарушение безопасности конфиденциальной информации».

Тем не менее, учитывая сложившуюся законотворческую практику России в сфере информационной безопасности, в рамках исследования настоящей статьи автор будет оперировать этими тремя терминами как тождественными.

Происходящие с начала 2022 г. политические и экономические драматические события очень сильно повлияли на формирование картины инцидентов нарушения безопасности конфиденциальной информации данных в мире и в России. На этом фоне очередной виток кибервойн спровоцировал всплеск кибератак и увеличение цены утечки персональных данных, коммерческой и государственной тайны, промышленных секретов, ноу-хау. Поэтому обеспечение безопасности конфиденциальной информации, выявление злоумышленников и предотвращение

инцидентов являются одними из самых актуальных задач для каждого государства в отдельности и мира в целом.

Учитывая вышесказанное, представляется актуальным провести анализ утечек данных за первое полугодие 2022 г. в России и мире. Экспертно-аналитический центр InfoWatch в своем отчете по итогам 2021 г. указывает, что «практически во всем мире примерно на 28 % произошло как снижение количества утечек, так и снижение количества скомпрометированных записей ПДн и платежной информации» [8]. Эксперты считают, что такие показатели были обусловлены комплексом факторов: «…рост латентности инцидентов (прежде всего внутреннего характера, т. е. по вине сотрудников), эффект от ранее внедренных DLP и других систем защиты, временное насыщение подпольного рынка данных (ДаркВеба), внимание этого рынка к обогащению ранее украденных баз данных, а также распространение вредоносного ПО, операторы которого в первую очередь нацеливаются не на кражу данных, а на их блокировку с целью получения выкупа» [7]. Ситуация кардинальным образом меняется в начале 2022 г., когда стал фиксироваться серьезный рост количества сообщений об инцидентах.

Эксперты аналитического центр InfoWatch указывают, что по итогам первой половины 2022 г. в мире зарегистрирована 2101 утечка информации ограниченного доступа, что почти в два раза (на 93,2 %) больше, чем за аналогичный период прошлого года. Количество утечек в России за первое полугодие 2022 г. составило 305 (+45,9 % по сравнению с I полугодием 2021 г.) [8]. Тем не менее в мире наблюдается тенденция к снижению утечек персональных данных и платежной информации. Так, за первые шесть месяцев 2022 г. в мире зафиксировано семь случаев утечки персональных данных, тогда как в первом полугодии 2021 г. таких инцидентов было десять, что на 27,8 % меньше единиц скомпрометированной информации. Но в России картина утечек персональных данных выглядит иначе. Количество инцидентов в первые шесть месяцев 2022 г. вырос в 16,75 раза и составил 187,6 млн записей [7].

Следует отметить, что переход на интернет-платформенное B2C взаимодействие принес много положительных изменений в коммерческие взаимоотношения между частными лицами и поставщиками. Так, для потребителей увеличился выбор товаров, работ и услуг, расширилась возможность приобретения по наиболее приемлемой цене, появился доступ 24/7 к рынку из любого места, при условии доступа к сети Интернет. Платформизация коммерческих взаимоотношений увеличила потребительскую аудиторию, что в свою очередь позитивным образом сказывается на прибыли бизнеса. Также благодаря интернет-платформам расширились способы и методы влияния на потребительский спрос через сбор и обработку сведений о предпочтениях и потребностях клиентов [1], составления «портрета» целевой аудитории на основе собранных и обработанных персональных данных. Повышенная коммерциализации персональных данных неизбежно приводит к увеличению их ценности и росту атак на их безопасность. Сказанное выше и разворачивающиеся драматические мировые и внутригосударственные события первой половины 2022 г. вполне объясняют, почему в этот период в России произошел всплеск утечки данных из российских компаний и госорганов, в их

числе: ОАО «РЖД», авиакомпания «Победа», телекоммуникационные компании «Ростелеком» и «ВымпелКом», информационный портал Ykt.ru, сервисы «Мир Тесен», Fotostrana.ru и Text.ru, развлекательный ресурс Pikabu, сервисы доставки «Яндекс.Еда», Delivery Club и 2 Berega, школа управления «Сколково», образовательный портал GeekBrains [7].

Далее представляется важным проанализировать виды нарушений, каналы и причины утечек информации в исследуемый период в сравнении с аналогичным периодом прошлого года в мире и России (см. табл.).

Соотношение долей нарушений по разным каналам утечек: Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г. [1]

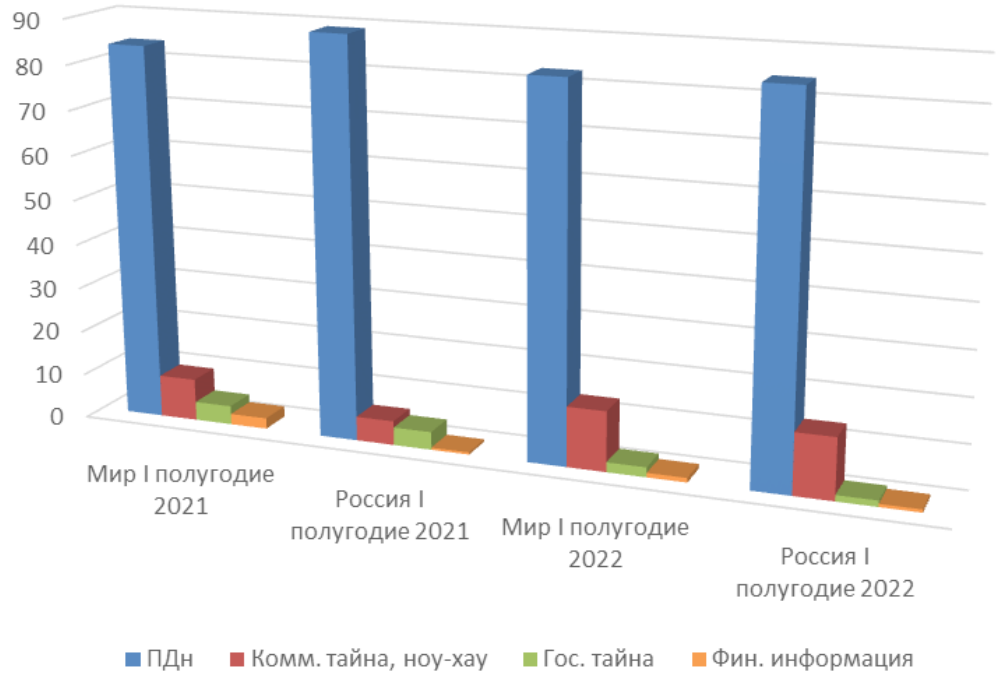
Вид нарушения	I полугодие 2021 г.		I полугодие 2022 г.	
	Мир, %	Россия, %	Мир, %	Россия, %
Внешние нарушители	60	21,5	90	81
Умышленные нарушения внешнего характера	83,2	86,4	97	96,3
Умышленные нарушения внутреннего характера	57,4	81,4	67	75,5

Как видно, доля инцидентов, спровоцированных действиями внешних нарушителей, в мире выросла на 30 %, а в России – почти на 60 %. Рост хакерских активностей вполне ожидаем. Одновременно с этим в мире поднялась доля умышленных нарушений внутреннего характера, тогда как в России эта доля упала примерно на 6 %.

Естественно, что в условиях повышенной хакерской активности и роста латентности внутренних нарушений самым распространенным каналом утечки данных является сеть Интернет. Второе место поделили электронная почта и сервисы мгновенных сообщений (IM). Доля бумажных носителей в этом антирейтинге резко упала.

Что же касается типов информации, наиболее подверженным неправомерным действиям, то картина в исследуемом периоде и в России, и в мире выглядит примерно одинаково: доминирующая доля принадлежит традиционно персональным данным, резко вырос процент утечек в промышленности и в сегменте «Торговля и HoReCa» (торговля и гостинично-ресторанный бизнес), тогда как в финансовом сегменте и госсекторе доля инцидентов нарушения безопасности данных немного снизилась, наблюдается также существенное снижение процента утечек в муниципальных органах власти и организациях.

Анализируя тенденцию спроса на конфиденциальную информацию, можно сделать следующие выводы. Снижение доли утечек персональных данных и рост утечек коммерческих секретов спровоцирован борьбой хакеров за сведения экономического характера, за государственные и оборонные секреты, ценные производственные сведения, клиентские базы торговых компаний, сетей отелей и общепита. И все-таки и в мире, и в России превалирующим типом информации на карте утечек информации остаются персональные данные: более 80 % от всех утечек (см. рис.) [7].



Распределение утечек по типам данных: Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г.

Анализ данных об инцидентах нарушения безопасности информации показывает, насколько сильно зависит этот сегмент информационных технологий от экономических и политических событий как в мире, так и внутри государства. «Интенсификация кибератак, развязывание новых кибервойн, широкое распространение хакерских инструментов и повышение значимости информации в мире, а также стремление ее использовать как инструмент шантажа, экономического и политического давления – все это привело к всплеску утечек, вызванных внешним воздействием» [7]. В России очень остро стоит вопрос обеспечения безопасности персональных данных на государственном уровне. Так, эксперты центра InfoWatch на основе анализа сообщений о продаже данных на теневых и «полутеневых» ресурсах, таких как форумы в ДаркВебе, а также в закрытых, анонимных Telegram-каналах пришли к выводу о процветании сегмента предоставления неправомерного доступа к персональным данным: «…ежедневно на подпольных форумах появляются десятки объявлений о продаже свежих баз данных, также злоумышленники предлагают (зачастую бесплатно или за символически деньги) базы из утечек прошлых лет» [8]. Надо отдать должное, на законодательном уровне регулярно предпринимаются шаги по усилению и расширению мер по защите персональных данных, ужесточению административной и уголовной ответственности за нарушение установленных правил обработки персональных данных. Например, Федеральным законом от 14.07.2022 № 266-ФЗ внесены масштабные изменения в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Вступившие с 1 сентября 2022 г. в силу новеллы затрагивают весь порядок работы с персональными данными: от согласия на обработку персональных дан-

ных и уведомления об инцидентах Роскомнадзора, ГосСопки до правил трансграничной передачи персональных данных, прекращения обработки персональных данных. За нарушение новых требований предусмотрена не только административная, но и уголовная ответственность (ст. 13.11, 13.12 и 19.7 КоАП РФ, ст. 137 и 272 УК РФ). Однако принятые новые меры не смогут помочь решить в должном объеме проблему защиты персональных данных от неправомерных действий, так как на законодательном уровне нет единого понимания понятийного аппарата. Как отмечалось выше, в российском законодательстве отсутствует целый ряд понятий: «утечка персональных данных», «утечка конфиденциальной информации», «инциденты нарушения безопасности конфиденциальной информации», «нарушение безопасности конфиденциальной информации», «инциденты нарушение безопасности персональных данных», «нарушение безопасности персональных данных» и др. Таким образом, без точной и ясной, закрепленной на высшем уровне правовой трактовки указанных терминов и понятий, которые будут использоваться в законодательных и иных нормативно-правовых документах, невозможно их практическое применение, единообразная и корректная квалификация правонарушений [6] в данной сфере, выработка универсальных стратегий по предотвращению инцидентов нарушения безопасности персональных данных и единых алгоритмов действий при обнаружении утечек (нарушения безопасности информации).

Учитывая изложенное, можно сделать вывод, что действующее законодательство в области информационной безопасности нуждается в унификации, выработке нового, отвечающего современным реалиям понятийного аппарата, а также в детализации и конкретизации существующих терминов и определений. Перечисленные шаги будут способствовать единому пониманию правовых норм всеми участниками правоотношений в сфере информационных технологий, защиты конфиденциальной информации, обработки персональных данных и т. п., а также ясному и прозрачному их толкованию, что, несомненно, благотворно отразится на справедливой квалификации незаконных деяний в данной области и применении адекватных мер воздействия к злоумышленникам.

Список литературы

1. Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3. С. 18–23.

2. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 11.09.2022).

3. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801./ (дата обращения: 11.09.2022).

4. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации» РС БР ИББС-2.9-2016: Приказ Банка России от 11.04.2016 № ОД-1205 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_197141/a5757a9d6b1316502aff9e53eb7d8ecb10690e96/ (дата обращения: 11.09.2022).

5. Роскомнадзор. Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных. URL: https://pd.rkn.gov.ru/incidents/ (дата обращения: 12.09.2022).

6. Черкасов В. Н. Информационная безопасность. Правовые проблемы и пути их решения // Информационная безопасность регионов. 2007. № 1 (1). С. 6–14.

7. Экспертно-аналитический центр InfoWatch. Отчет об исследовании утечек информации ограниченного доступа в I половине 2022 года. URL: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения: 11.09.2022).

8. Экспертно-аналитический центр InfoWatch. Отчет об исследовании утечек информации ограниченного доступа в 2021 году. URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (дата обращения: 11.09.2022).

9. Guidelines 01/2021 on Examples regarding Data Breach Notification. 2021, January. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf (дата обращения: 15.09.2022).

Н. С. Золотарев,
аспирант,
Московский финансово-юридический университет

ЦИФРОВАЯ ЭКОНОМИКА, ЦИФРОВОЕ ПРАВО И ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО

Аннотация. Движение жизни вперед выводит нас на качественно новые уровни, назначение которых – улучшение условий существования людей. Одно из таких качественных изменений – цифровизация, проникающая во все сферы: экономику, культуру и право. В российской экономико-правовой сфере цифровизация – обстоятельство сравнительно «новое». Хотя между государственно-частным партнерством и «цифровыми» экономикой с правом существуют достаточно большие «дистанции», представляется, что цифровизация различных сфер общественной жизни «нуждается» в значительных инвестиционных вложениях, а разумное и эффективное распределение вложенных средств должно осуществляться с участием государства.

Ключевые слова: цифровизация, цифровая экономика, цифровое право, государственно-частное партнерство

DIGITAL ECONOMY, DIGITAL LAW AND PUBLIC-PRIVATE PARTNERSHIPS

Abstract. The movement of life forward brings us to qualitatively new levels, the purpose of which is to improve the living conditions of people. One of such qualitative changes is digitalization, “penetrating” into all areas – economy, culture and law. In the