Никифоровская Диана Вадимовна,
студентка ОГБПОУ
«Колледж индустрии питания,
торговли и сферы услуг»,
г. Томск

Дозморова Татьяна Васильевна,
преподаватель ОГБПОУ
«Колледж индустрии питания,
торговли и сферы услуг»,
г. Томск

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННО–КОММУНИКАЦИОННЫХ СЕТЯХ

УДК 347.77

В условиях активного развития информационных технологий важной проблемой становится умение применять различные способы обеспечения безопасности персональных данных. Автор уверен, что одним из наиболее эффективных методов решения проблемы является постоянный контроль своих персональных данных в информационной среде и знание законодательной базы.

In the context of the active development of information technology, the ability to use various methods to ensure the security of personal data becomes an important problem. The author is confident that one of the most effective methods of solving the problem is constant monitoring of one's personal data in the information environment and knowledge of the legislative framework.

Ключевые слова: безопасность, персональные данные, информационно-коммуникационные сети.

Keywords: security, personal data, information and communication networks.

В современном мире, когда информационные технологии являются неотъемлемой частью нашей жизни, частная жизнь человека, его персональные данные подвергаются огромному риску попасть в руки мошенников. Многие, не задумываясь, оставляют свои фотографии и личные данные в социальных сетях, при переписке, не заботятся о важности пароля, перемещаются на незнакомые сайты и т. д. Когда человек вводит информацию о себе, оператор персональных данных обязуется обработать и хранить их, как того требует Закон «О персональных данных». В том числе не передавать эту информацию кому-то еще, если пользователь не давал разрешения. Если персональные данные попадают в открытый доступ, оператор несет административную ответственность. Причем неважно, кто виноват. В результате ошибки или намеренного действия оператора информация может попасть в руки мошенников. Поэтому правильно вести себя в мире информационных технологий и знать опасности и способы защиты является актуальным для любого человека. Гипотезой работы будет предположение, что современная

законодательная база защищает персональную информацию пользователей РФ. Цель работы – изучить риски, которым могут подвергаться пользователи Интернета, и законодательные способы защиты персональных данных. В условиях активного развития информационных технологий важной проблемой становится умение применять различные способы обеспечения безопасности персональных данных. Одним из наиболее эффективных методов решения проблемы является постоянный контроль своих персональных данных в информационной среде и знание законодательной базы.

ЗАКОНОДАТЕЛЬНАЯ БАЗА ПО ПЕРСОНАЛЬНЫМ ДАННЫМ

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1.1 введен Федеральным законом от 30.12.2020 № 519-ФЗ) [1].

За нарушение закона о персональных данных ждет штраф. Основной закон по работе с персональными данными – Федеральный закон от 27.07.2006 № 152-ФЗ [1]. Он определяет, что относится к персональным данным и правила работы с ними. За нарушение закона предусмотрена гражданско-правовая, административная и даже уголовная ответственность.

В последние годы в связи с резким скачком информационных технологий, участившимися случаями утечек данных у российских компаний и повышенными киберрисками в текущих реалиях происходят и изменения на законодательном уровне. В первую очередь, меняются подходы к порядку обработки и защиты персональных данных, что затрагивает деятельность как российских, так и иностранных компаний.

К наиболее существенным нововведениям относятся:

- распространение действия Закона № 152-ФЗ на иностранные компании, обрабатывающие персональные данные российских граждан;
- новые правила трансграничной передачи данных, которые фактически вводят разрешительный порядок трансграничной передачи, а также обязывают операторов проводить оценку получателей данных за границей;
- обязанность операторов уведомить Роскомнадзор об утечках персональных данных;
- взаимодействие операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА);
- необходимость подготовки более детальных политик обработки персональных данных;
- сокращение сроков ответа на запросы субъектов персональных данных.

АНАЛИЗ ПРЕСТУПЛЕНИЙ

По данным МВД, за 2023 год выросло количество преступлений с использованием интернета: с 381,1 тысячи до 526,7 тысячи. На втором и третьем местах оказались мошенничества, совершенные с применением средств мобильной связи и пластиковых карт. Также участились правонарушения с использованием компьютерной техники, программных средств и фиктивных электронных платежей [3].

Наибольший темп прироста противоправных деяний, совершенных с помощью информационных технологий, отмечен в Ненецком автономном округе, Калмыкии, Новгородской и Калининградской областях, а также в Ингушетии. Наибольшее число инцидентов связано с заражением вредоносным программным обеспечением (далее – ПО) через посещение сайтов с вредоносным контентом и фишинговые атаки. В 2023 году Роскомнадзор зарегистрировал 168 утечек персональных данных, из-за которых в открытый доступ попало больше 300 млн записей о россиянах.

В 2022 году эксперты в сфере кибербезопасности зафиксировали 710 случаев умышленной утечки информации – вдвое больше, чем в 2021 году. Общее количество утекших данных – 667,6 млн записей. Обычно каждая запись – это информация об одном пользователе. По данным исследования, которое провела компания по предотвращению и расследованию киберпреступлений F.A.C.C.T., сейчас на российских серверах в открытом доступе находится около 7500 баз данных [4].

Согласно источнику InfoWatch, чаще всего в открытом доступе оказываются именно персональные данные: в 2022 году на их долю приходилось почти 88,9%. На втором месте – коммерческие тайны, на третьем – государственные тайны. Реже всего в открытый доступ попадает платежная информация, то есть данные банковских карт. В 2019 году зарегистрировали 360 случаев умышленной утечки данных, а уже в 2020 году – 464 – участились мошеннические схемы, связанные с вакцинацией, QR-кодами и социальными выплатами [2].

Кроме того, во время пандемии выросло количество самих источников персональных данных, прежде всего медицинского характера: базы заразившихся коронавирусом и информация о вакцинированных. Например, в декабре 2020 года в открытом доступе появились данные 100 тысяч москвичей, переболевших COVID-19. Также выросли объемы баз различных сервисов, в первую очередь связанных с доставкой. Например, 1 марта 2022 года стало известно о крупной утечке данных сервиса «Яндекс.Еда», а за день до этого о подобном происшествии заявили в сервисе доставки СДЭК *(рис. 1)*.

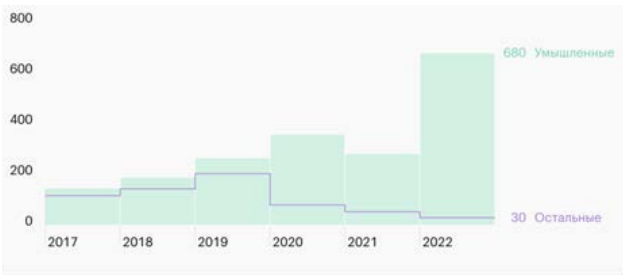

Рис. 1. Количество утечек данных

Если в 2018 году в России преобладали утечки из-за

кражи документов или их утери, то в последующие годы резко выросла доля случаев, когда информация хранилась в интернете и мессенджерах – исследователи разделяют эти источники. В первой половине 2022 года большинство данных утекло именно через интернет: 92,8% от всех происшествий. На втором месте – мессенджеры: 3,2% утечек. На третьем и четвертом – электронная почта и бумажные документы: 2,8 и 0,8% соответственно [6].

Виновниками утечек чаще всего становятся хакеры и неизвестные лица – на их долю приходится 89,8% всех утечек. Хакерские атаки часто происходят из-за того, что многие сервисы, где пользователи регистрируются с собственным паролем, используют для хранения паролей устаревшие алгоритмы или вовсе хранят их в открытом текстовом виде. Международный союз электросвязи составляет глобальный индекс кибербезопасности – Global Cybersecurity Index (GCI). Самый высокий показатель по итогам 2020 года – у США: 100 пунктов. Россия занимает в списке восьмое место с показателем 98,06. Еще два года назад наша страна находилась на 29-й строчке, результат 2020 года – это максимальное значение за все время публикации индекса.

Массовые утечки почти 300 млн пользовательских данных в 2022 году, затронувшие крупнейших игроков на рынке («Яндекс.Еда», СДЭК, Delivery Club, «Гемотест», «Ростелеком», «Почта России», Tele2 и пр.), активно использовались злоумышленниками в 2023 году для проведения атак. Чувствительные данные обнаруживаются в 98,5% случаев поиска по целевой компании (48% учетных записей содержат связку логин-пароль, 44% учетных записей упоминаются в связке с хэшем пароля). Сотрудники чаще всего оставляют корпоративные почтовые адреса в сервисах медицинских клиник, а также в интернет-магазинах.

По сведениям Банка России, в 2022 году от инвесторов и потребителей финансовых услуг поступило 386 тыс. жалоб. При этом участились случаи мошеннических действий в отношении граждан, в том числе связанных с оформлением займов от имени лиц, которые договор займа не заключали (+ 38,6% в сравнении с 2021 годом). Больше всего операций без согласия клиентов – физических лиц пришлось на оплату покупок в интернете. Клиенты банков сообщили о 515,88 тыс. таких операций, 48,7% из которых – результат применения к ним приемов и методов социальной инженерии. Сумма хищений составила 2550,54 млн руб. *(рис. 2)*.

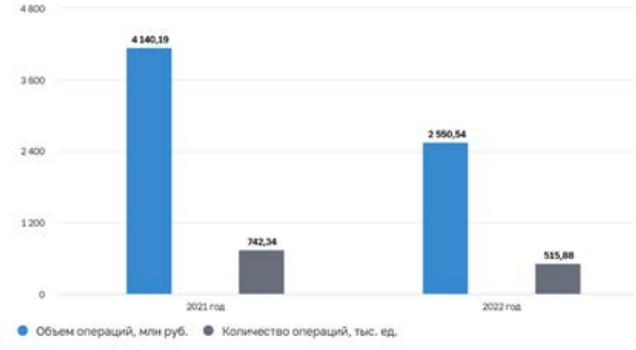

Рис. 2. Операции без согласования клиентов при оплате товаров и услуг в интернете

В течение 2022 года операторами связи было заблокировано более 4 млн вызовов (в два раза больше относительно показателя 2021 года), которые пытались осуществить злоумышленники с использованием технологии подмены номера *(рис. 3)*.

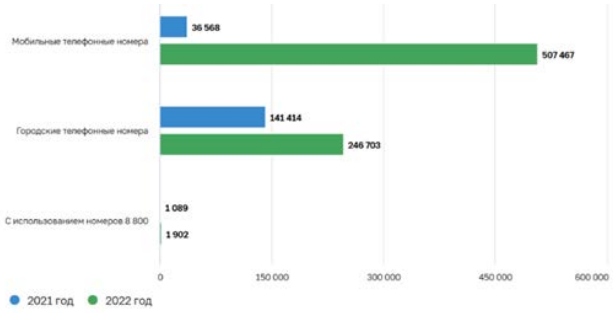

Рис. 3. Использование мошеннических телефонов

Кроме того, Банк России направил в адрес регистраторов доменных имен запросы на проведение проверочных мероприятий и снятие с делегирования 5217 доменных имен Сети, с использованием которых осуществлялась противоправная деятельность *(рис. 4-5)*.

Рис. 4. Типы ресурсов, используемые злоумышленниками в 2022 г.

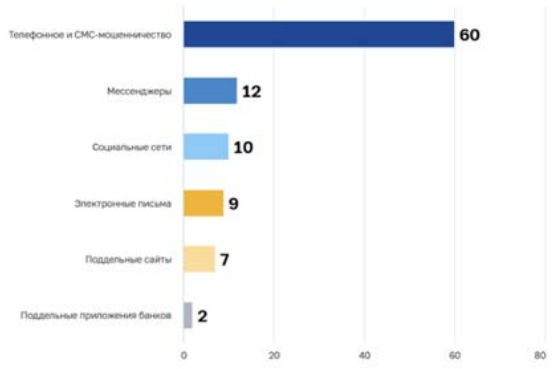

Рис. 5. Каналы мошенничества

Согласно статистике МВД России, за 2022 год зарегистрировано 522 тыс. преступлений, совершенных в сфере информационно-телекоммуникационных технологий и компьютерной информации, что на 0,8 % больше, чем в 2021 году. Больше половины преступлений в цифровой среде (52,1%) составляют тяжкие и особо тяж-

кие (272,2 тыс.). Около трех четвертей (73,0%) совершаются с использованием интернета – 381,1 тыс. (+8,4%). Более трети (213 тыс., или 40,8%) совершено с использованием средств мобильной связи [6].

Почти три четверти преступлений, совершенных в сфере информационно-телекоммуникационных технологий и компьютерной информации, составляют кражи и мошенничества (371,2 тыс., или 71,1%).

При этом по сравнению с 2021 годом уменьшилось количество преступлений, предусмотренных статьей 273 УК РФ, – создание, использование и распространение вредоносных компьютерных программ *(рис. 6)*.

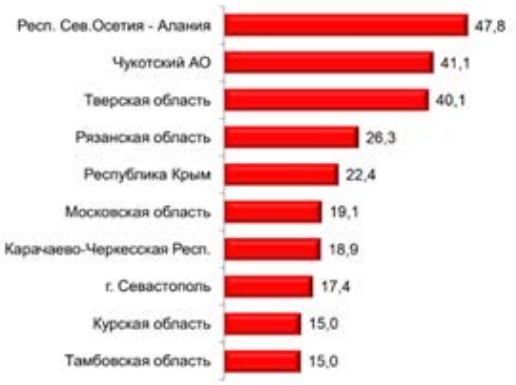

Рис. 6. Регионы с наибольшими темпами прироста зарегистрированных преступлений, %

По данным Генеральной прокуратуры, в сфере информационно-телекоммуникационных технологий и компьютерной информации зарегистрировано 6 141 преступление в отношении несовершеннолетних, 2 647 из которых направлены в суд с обвинительным заключением. В отношении пенсионеров в 2022 году совершены 59 949 преступлений [7].

В 2022 году зарегистрировано 862 преступления, предусмотренных статьей 137 УК РФ, – нарушение неприкосновенности частной жизни, 572 из которых направлены в суд с обвинительным заключением.

Финансовые организации также создают и развивают сервисы, направленные на проверку сомнительных телефонных номеров и сайтов. По оценке РКН, обработку ПД граждан на территории России осуществляет свыше 6 млн организаций и индивидуальных предпринимателей, общее количество баз ПД, с которыми работают эти операторы, превышает 3 млн. Фактически, по оценкам экспертов, о каждом гражданине РФ, в зависимости от его активности в Сети, содержатся записи в среднем от 10 до 100 и более базах данных. В общей сложности это почти 13 млрд записей с персональными данными наших граждан.

В 2023 году из банков и финансовых компаний утекло 170,3 млн записей персональных данных клиентов – больше, чем население России, подсчитали в InfoWatch. За год их число выросло в 3,2 раза. Всего российские финансовые организации допустили 64 случая потери персональных данных клиентов, что превышает показатели 2022 года на 12,3%, а 2021 года – почти вдвое. Примерно половина утечек – 46,9% – пришлась на банки. С компрометацией данных клиентов также сталкиваются микрофинансовые организации (далее – МФО), платежные сервисы, криптобиржи, традиционные биржи, инвестиционные компании и другие участники финансового рынка.

Всего, согласно данным Роскомнадзора, в 2023 году суды рассмотрели 87 составленных ведомством протоколов по факту утечек персональных данных и назначили штрафы на общую сумму более 4,6 млн рублей. В июне 2023 года замглавы Роскомнадзора Милош Вагнер сообщил ТАСС, что с начала года произошло более 70 утечек персональных данных, в сеть попали порядка 200 млн записей о россиянах [8]. Хотя полностью защитить информацию о себе невозможно, так как субъект персональных данных практически никогда не контролирует их обработку, единственное, что можно сделать, – максимально разделить эти данные, чтобы затруднить обогащение различных баз с их помощью, быть внимательными и вовремя обращаться в государственные органы.

Таким образом, рассмотрев риски, которым могут подвергаться пользователи Интернета, и законы по защите персональных данных, а также статистику правонарушений в данной области, можно сделать вывод, что при правильном обращении со своей информацией и соблюдении закона можно обезопасить свои персональные данные от действий мошенников.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.: сайт. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=447363 (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

2. База данных российской судебной практики по информационному праву: сайт. – URL: https://4people.grfc.ru/analytics-and-legislation/case-studies/obzor-moshennichestva-s-personalnymi-dannymi-grazhdan-v-cifrovoy-srede-vtoroe-polugodie-2022-g / (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

3. Министерство внутренних дел РФ: сайт. – URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения 27.10.2023). – Режим доступа свободный. – Текст электронный.

4. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года: сайт. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

5. РАПСИ: Российское агентство правовой и судебной информации: сайт. – URL: https://rapsinews.ru/digital_law_news/20240312/309690643.html/ (дата обращения 27.01.2024).– Режим доступа свободный. – Текст электронный.

6. Судебная практика по спорам о защите персональных данных. Сайт: https://ppt.ru/news/138028 (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

7. Статистика и аналитика: сайт. – URL: https://xn-

-b1aew.xn--p1ai/dejatelnost/statistics (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

8. Федеральная служба по надзору в сфере связи: отчет о деятельности уполномоченного органа по защите прав субъектов персональных данных за 2019 год информационных технологий и массовых коммуникаций, отчет о деятельности уполномоченного органа по защите прав субъектов персональных данных за 2019 год: сайт. – URL: https://rkn.gov.ru/docs/Otchet_UO-2019_new.pdf (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.

9. Центр правовой помощи гражданам в цифровой среде: сайт. – URL: https://4people.grfc.ru/analytics-and-legislation/case-studies/obzor-moshennichestva-s-personalnymi-dannymi-grazhdan-v-cifrovoy-srede-vtoroe-polugodie-2022-g / (дата обращения 27.01.2024). – Режим доступа свободный. – Текст электронный.