Научная статья
УДК 349.681
DOI: 10.37973/VESTNIKKUI-2024-56-7

БОРЬБА С УТЕЧКАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ – ПОМОЖЕТ ЛИ УЖЕСТОЧЕНИЕ ОТВЕТСТВЕННОСТИ?

Алексей Николаевич Прокопенко,
Академия Государственной противопожарной службы
МЧС России, Москва, Россия,
Alex_prokop@rambler.ru

Аннотация

Введение: в статье рассматриваются массовые кибератаки на информационную инфраструктуру России. Указывается, что одной из основных целей преступников являются информационные системы персональных данных.

Обзор литературы: в ходе исследования анализировались научные труды А.В. Минбалеева, Л.К. Терещенко, М.Б. Добробабы, П.А. Виноградовой, Ю.Н. Мильшина, С.Г. Чубуковой и др., а также последние изменения законодательства о персональных данных.

Материалы и методы: в ходе исследования использовались системный метод, а также формально-юридический, сравнительно-правовой и конкретно-социологический методы. Эмпирическими данными выступили российские нормативные правовые документы, статистические исследования, а также научные работы по теме исследования.

Результаты исследования: анализируются внесенные в июле 2022 года изменения в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», имевшие, в том числе, своей целью уменьшить количество утечек, повысить количество выявленных киберинцидентов и отраженных атак. Отмечается, что в десятки раз увеличилось количество операторов персональных данных, которые должны сообщать в Роскомнадзор о том, что они обрабатывают персональные данные. Полноценное оформление обработки персональных данных и защита информационных систем персональных данных вызывают существенные затруднения у «новых» операторов. Ситуация усугубляется кадровым некомплектом. Также анализируются положения, в соответствии с которыми осуществляется реагирование на инциденты, связанные с утечками персональных данных, и информирование о них ФСБ России и Роскомнадзора.

Обсуждение и заключение: делается вывод о сложности исполнения принятых изменений законодательства малыми и средними компаниями, в том числе муниципальными организациями. Указывается на проблемы, возникшие в связи с изменениями, внесенными в законодательство, и ожидаемым введением норм административной ответственности за их неисполнение. Предлагаются пути решения возникших проблем, в том числе создание массовых программ по обучению сотрудников операторов персональных данных, создание специальных облачных платформ для защиты персональных данных, обрабатываемых в организациях, отложение введения норм административной ответственности для малого бизнеса сроком на один год.

Ключевые слова: персональные данные; информационные системы персональных данных; киберинциденты; утечки персональных данных; малый бизнес; средний бизнес; административная ответственность

© Прокопенко А.Н., 2024

Для цитирования: Прокопенко А.Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 48 – 56. DOI: 10.37973/VESTNIKKUI-2024-56-7

Scientific article
UDC 349.681
DOI: 10.37973/VESTNIKKUI-2024-56-7

COMBATING PERSONAL DATA LEAKS – WILL TIGHTENING LIABILITY HELP?

Alexey Nikolaevich Prokopenko,
the Academy of the State Fire Fighting Service
of the Ministry of Emergency Situations of Russia, Moscow, Russia,
Alex_prokop@rambler.ru

Abstract

Introduction: the article examines mass cyberattacks on the Russian information infrastructure. It is indicated that one of the main goals of criminals is personal data information systems.

Literature review: the research analyzed the scientific works of A.V. Minbaleev, L.K. Tereshchenko, M.B. Dobrobaba, P.A. Vinogradova, Yu.N. Milshina, S.G. Chubukova and others, as well as recent changes in the legislation on personal data.

Materials and Methods: the study employed a systematic methodology, integrating legal, comparative-legal, and sociological approaches. The empirical data consisted of legal acts of the Russian Federation, statistical studies, and scientific works.

Results: the changes made in July 2022 to the Federal Law "On Personal Data" which, among other things, had the goal of reducing the number of leaks, increasing the number of identified cyber incidents and repulsed attacks, are analysed. It is noted that the number of personal data operators who must report to Roskomnadzor that they are processing personal data has increased tenfold. The comprehensive design of the processing of personal data and the protection of personal data information systems present significant challenges for "new" operators. These challenges are further compounded by the lack of trained personnel. The provisions pertaining to the response and notification of incidents related to personal data leaks are also analysed. These provisions stipulate that the FSB of Russia and Roskomnadzor are responsible for responding to and informing the public about such incidents.

Discussion and Conclusions: it is concluded that the implementation of the adopted changes in legislation by small and medium-sized companies, including municipal organisations, is challenging. This indicates the problems that have arisen in connection with the changes made to the legislation and the expected introduction of norms of administrative responsibility for their failure to comply. A number of potential solutions to the issues that have arisen are put forward, including the establishment of comprehensive training programmes for employees of data processors, the creation of dedicated cloud platforms for the protection of personal data processed by small and medium-sized organisations, and the postponement of the introduction of administrative responsibility standards for small businesses for a year.

Keywords: personal data; personal data information systems; cyber incidents; personal data leaks; small and medium-sized businesses; administrative responsibility

© Prokopenko A.N., 2024

For citation: Prokopenko A.N. Combating Personal Data Leaks – Will Tightening Liability Help? Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(2):48-56. (In Russ.). DOI: 10.37973/VESTNIKKUI-2024-56-7

Введение

Сохранность персональных данных граждан России является одной из значительных социальных и экономических проблем в настоящее время. Частые кибератаки на критическую инфраструктуру Российской Федерации не прекращаются в течение последних двух лет. Причем данные кибератаки приобрели массовый характер и координируются иностранными спецслужбами. Одним из объектов для кибератак являются базы персональных данных. Согласно исследованию компании SearchInform за 2022 год, персональные данные становились одной из целей преступников в 52% кибератак на государственные органы и организации, а также в 28% кибератак на коммерческие организации[1]. Количество кибератак на информационные системы персональных данных в 2023 году только увеличилось [1]. Также большое количество утечек происходит из-за халатности сотрудников организаций,

[1] Исследование уровня информационной безопасности в компаниях России за 2022 год. URL: https://searchinform.ru/survey/global-2022/ (дата обращения: 08.10.2023).

недостаточно ответственного подхода руководства организаций к организации защиты данных [2]. Таким образом, изменение законодательства о персональных данных, в том числе повышение ответственности за утечки данных, представляется одним из способов обеспечения информационной безопасности.

Изменения в статью 13.11 КоАП РФ приняты Государственной Думой Российской Федерации в первом чтении, обсуждаются в настоящее время и могут быть скорректированы по результатам научных исследований.

Целью исследования является анализ двух взаимосвязанных направлений изменения законодательства о персональных данных:

- принципиальное изменение подхода к обработке персональных данных для операторов персональных данных, стимулирующее увеличение в десятки раз количества операторов персональных данных, которые должны сообщать в Роскомнадзор о том, что они обрабатывают персональные данные;

- добавление в закон положений о реагировании организаций на инциденты, связанные с утечками персональных данных, которое привело к необходимости создания в организациях подразделений информационной безопасности.

Обзор литературы

Вопросы правового регулирования обработки персональных данных, в том числе после новейших изменений законодательства, неоднократно становились предметом научного исследования в трудах А.В. Минбалеева, Л.К. Терещенко, М.Б. Добробабы, П.А. Виноградовой, Ю.Н. Мильшина, С.Г. Чубуковой и др. [3 – 9]. Вместе с тем проблема соотношения изменений, внесенных в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), планирующихся изменений в статью 13.11 КоАП РФ и возможностей организаций по выполнению новых норм закона требует дополнительного исследования.

Материалы и методы

Основой исследования являлся системный метод. Кроме того, в рамках исследования применялись формально-юридический, сравнительно-правовой и конкретно-социологический методы. Эмпирическими данными выступили российские нормативные правовые документы, статистические исследования, а также научные работы по теме исследования.

Объединение исследуемых данных, установление общих закономерностей и связей позволило выявить корреляционные взаимодействия и влияния нормативных правовых актов на реальную ситуацию. В целом применение различных научных методов обеспечило воплощение требований системного, ситуационного и комплексного подходов анализа исследуемых общественных отношений.

Результаты исследования

В июле 2022 года Федеральным законом от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»[1] были внесены существенные изменения в ФЗ «О персональных данных»[2], направленные, в том числе, на защиту баз данных персональных данных от утечек и кибератак [4, с. 203 – 214]. Данные изменения осуществлялись по двум направлениям.

Первым направлением является принципиальное изменение подхода к обработке персональных данных для операторов персональных данных.

Многие операторы эксплуатировали информационные системы персональных данных, но не соблюдали должным образом требования законодательства. Часть 2 статьи 22 ФЗ «О персональных данных» ранее предусматривала, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных. Например, не были обязаны направлять уведомления работодатели, которые обрабатывали персональные данные своих сотрудников в трудовых целях, а также общественные и религиозные организации, обрабатывавшие персональные данные своих членов. Кроме того, обязанность направлять уведомления об обработке персональных данных не распространялась на фирмы, которые собирали персональные данные клиентов для заключения договоров на продажу товаров, выполнения работ или оказания услуг [5].

К указанным трем видам организаций относится большая часть юридических лиц в России, которые до 1 сентября 2022 года не уведомляли Роскомнадзор, соответственно, не подвергались проверкам на соблюдение законодательства о персональных данных. Аналогично не подверга-

[1] О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»: Федеральный закон от 14.07.2022 № 266-ФЗ // Российская газета. № 156-157 (дата обращения: 20.07.2022).

[2] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ. URL: http://pravo.gov.ru (дата обращения: 06.02.2023).

лась проверкам значительная часть государственных и муниципальных организаций.

Все указанные юридические лица и ранее являлись операторами персональных данных и были обязаны оформлять весь комплект документов, предусмотренный законодательством, а также обеспечивать защиту информационных систем. Однако большая часть из них соблюдала законодательство фрагментарно. Например, в организации брали согласие физического лица на предоставление его персональных данных при приеме на работу и осуществляли защиту информационных систем, в которых указанные данные обрабатывались и хранились, но не принимали Политику в отношении обработки персональных данных, не назначали ответственного за обработку персональных данных, не осуществляли внутренний контроль за обработкой персональных данных; то есть не полностью соблюдали требования статей 18.1 и 19 ФЗ «О персональных данных».

Вторым направлением изменений Федерального закона «О персональных данных» стало добавление в закон положений о реагировании организаций на инциденты, связанные с утечками персональных данных.

Статья 19 Закона была дополнена частями 12-14, которые ввели совершенно новые обязанности для операторов. Так, операторы персональных данных теперь обязаны сотрудничать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [6]. Операторы должны информировать Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных (далее – инцидент), на основании приказа ФСБ России от 13.02.2023 № 77[1].

Статья 21 ФЗ «О персональных данных» также дополнена частью 3.1, которая обязала оператора после инцидента, приведшего к утечке персональных данных, извещать Роскомнадзор. Во-первых, оператор должен в течение 24 часов сообщить в Роскомнадзор о произошедшем инциденте, причинах его возникновения, вреде и принятых мерах по его устранению. Кроме того, оператор должен предоставить Роскомнадзору контакты лица, которое уполномочено на расследование инцидента, для дальнейшего взаимодействия. Во-вторых, оператор обязан провести внутреннее расследование и сообщить в Роскомнадзор о виновных лицах в течение 72 часов после инцидента.

Приказ ФСБ России от 13.02.2023 № 77 в пункте 2 указывает, что информирование через НКЦКИ осуществляется только операторами, которые подключены к Центру и, соответственно, к ГосСОПКА. Это преимущественно организации, эксплуатирующие объекты критической информационной инфраструктуры, финансовые компании, банки, операторы связи, интернет-провайдеры и т.д. Все организации, которые не взаимодействуют с НКЦКИ, обязаны об инцидентах извещать Роскомнадзор на основании положений статьи 21 ФЗ «О персональных данных» и пункта 3 данного приказа.

Кроме того, статья 23 ФЗ «О персональных данных» была дополнена частями 10 и 11, которые установили обязанность Роскомнадзора вести Реестр учета инцидентов в области персональных данных и взаимодействовать с ГосСОПКА в рамках обмена информацией об инцидентах. Аналогичный реестр ведется в НКЦКИ, а инцидент считается зарегистрированным после присвоения ему идентификатора (пункт 4 приказа ФСБ России от 13.02.2023 № 77).

Взаимодействие регулятора с операторами для ведения Реестра осуществляется в соответствии с приказом Роскомнадзора от 14.11.2022 № 187[2]. Между НКЦКИ и Роскомнадзором также организован обмен информацией об инцидентах.

Анализ вышеуказанных изменений позволяет сделать следующие выводы.

Во-первых, количество операторов персональных данных, которые обязаны направлять уведомление об обработке персональных данных в Роскомнадзор, увеличилось в десятки раз. При этом изменение порядка проведения контрольно-надзорных мероприятий Роскомнадзором на основе риск-ориентированного подхода[3] позволит ему осуществлять кратно большее количество проверок.

[1] Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных: приказ ФСБ России от 13.02.2023 № 77. URL: http://pravo.gov.ru (дата обращения: 20.02.2023).

[2] Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных: приказ Роскомнадзора от 14.11.2022 № 187. URL: http://pravo.gov.ru (дата обращения: 28.12.2022).

[3] О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации: Федеральный закон от 11.06.2021 № 170-ФЗ // Российская газета. № 133 (дата обращения: 18.06.2021).

Данное направление деятельности является новым для большинства организаций, вызывает затруднения, а часть из них до сих пор не знает о своих обязанностях. Внесенные изменения фактически назвали операторами все организации в России и обязали их вести весь комплект документации об обработке персональных данных, соблюдать требования постановления Правительства Российской Федерации от 21.03.2012 № 211 (для государственных и муниципальных организаций)[1], постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[2], постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»[3], а также подзаконных актов Роскомнадзора, ФСТЭК России и ФСБ России.

Для устранения возникающих затруднений требуется организация обучения представителей операторов, которые раньше не должны были информировать Роскомнадзор об обработке персональных данных. Обучение технических специалистов организовано ФСТЭК России и ведется уже более десяти лет, а обучение сотрудников кадровых и финансовых подразделений полноценно не организовано ни в государственном, ни в частном секторе. При этом общее количество нетехнических специалистов, которых требуется обучить правильной обработке персональных данных, составляет несколько десятков тысяч человек. В отдельных министерствах, субъектах РФ и крупных компаниях, например в МЧС России, обучение основам обработки персональных данных ведется, но широкого распространения данная практика не получила.

Во-вторых, анализ внесенных изменений и указанных документов позволяет сделать вывод о чрезмерности принятых требований.

Приказ ФСБ России от 13.02.2023 № 77 в пунктах 2 и 3 четко разделяет всех операторов персональных данных на две группы. Те, кто сотрудничает с НКЦКИ, должны информировать ФСБ России, а те, кто не сотрудничает, должны извещать об инцидентах Роскомнадзор. Однако закон в статье 21 таких ограничений не установил и обязал всех операторов извещать о произошедших инцидентах. В результате операторы, которые являются владельцами объектов критической информационной инфраструктуры, должны осуществлять двойное информирование.

Кроме того, установленные сроки информирования об инцидентах, а также об их расследованиях возможно соблюсти только операторам – крупным организациям, которые имеют в своем составе развитую службу информационной безопасности. Как правило, к ним относятся владельцы объектов критической инфраструктуры, федеральные министерства и ведомства в целом. Остальные организации, даже при выявлении инцидента, не смогут расследовать его за 72 часа и, скорее всего, нарушат закон, то есть не осуществят информирование в указанные сроки.

В результате для малых и средних операторов персональных данных, к которым относятся 99% российских организаций, выполнение указанных требований представляется трудноисполнимым. Не каждая компания, которая занимается онлайн-торговлей и в которой работает до 100 сотрудников, сможет самостоятельно выявить компьютерный инцидент, который привел к утечке персональных данных клиентов. В подавляющем большинстве случаев указанная компания даже не определит, что ее взломали, поскольку полноценная защита информации, работа службы информационной безопасности и лицензия на программное обеспечение для выявления инцидентов стоит несколько миллионов рублей в год. И совершенно точно компания не будет знать, что делать после инцидента, как расследовать, как определять ущерб и т.д. Соответственно, требования статьи 21 ФЗ «О персональных данных» будут не выполнены.

Указанные положения закона также вызывают существенные затруднения у государственных и муниципальных организаций. Однако в этом случае есть возможность сосредоточить функции выявления инцидентов на уровне центрального аппарата министерств и ведомств или на уровне правительства субъекта РФ. Особенно трудности

[1] Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: постановление Правительства Российской Федерации от 21.03.2012 № 211. URL: http://www.pravo.gov.ru (дата обращения: 17.04.2019).

[2] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Российской Федерации от 01.11.2012 № 1119 // Российская газета. № 256 (дата обращения: 07.11.2012).

[3] Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства Российской Федерации от 15.09.2008 № 687 // Российская газета. № 200 (дата обращения: 24.09.2008).

будут испытывать операторы, которые ранее не должны были уведомлять Роскомнадзор об обработке персональных данных. Теперь они должны не только осуществлять полное документальное сопровождение обработки персональных данных, но и обеспечивать полноценную защиту информационных систем персональных данных. Однако большинство компаний для этого не располагают денежными средствами.

Негативная ситуация для малых и средних компаний, а также муниципальных организаций, усугубляется скорым принятием изменений в статью 13.11 КоАП РФ[1], устанавливающих ответственность за нарушения законодательства о персональных данных [10]. В соответствии с проектом Федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[2] планируется установить ответственность за неуведомление Роскомнадзора об обработке персональных данных (до 150 тыс. рублей на юридических лиц) и за неуведомление Роскомнадзора об утечках в результате инцидента (до 3 млн рублей на юридических лиц). Кроме того, в частях 12 – 14 измененной статьи 13.11 КоАП РФ планируется установить ответственность оператора за действия или бездействия, которые привели к инциденту и утечке. Ответственность будет наступать за утечку более 1000 персональных данных субъектов или более 10 тысяч уникальных обозначений сведений о физических лицах, необходимых для определения таких лиц. Штрафные санкции для юридических лиц составляют от трех млн рублей и до 500 млн рублей при повторном нарушении и крупномасштабных утечках.

В результате внесения таких изменений в КоАП РФ большая часть компаний, оказывающих услуги или продающих товары с использованием информационных систем через Интернет, должна будет закрыться для того, чтобы не попасть под угрозу штрафа размером в несколько миллионов рублей. Ведение бизнеса без инцидентов в условиях постоянных кибератак из-за границы является фактически невозможным, а выполнение требований ФЗ «О персональных данных», как было указано выше, трудноисполнимым. Для корректировки возможных последствий от законопроекта представители малого и среднего бизнеса обратились в Государственную Думу Российской Федерации с просьбой уменьшить штрафы или отложить срок введения ответственности[3].

Представляется, что требуется не только отложить для малых и средних компаний, а также для муниципальных организаций, вступление изменений в статью 13.11 КоАП РФ минимум на один год, но и принять ряд других правовых и организационных мер.

Отмена внесенных изменений в Федеральном законе «О персональных данных», предусматривающих информирование в результате утечек персональных данных, представляется нецелесообразной, особенно в современных условиях. Однако поскольку полноценная защита персональных данных в информационных системах и выявление инцидентов недоступны для малых субъектов, то требуется создание таких организационных и технических условий, которые уменьшат утечки, но не разрушат бизнес. Решением указанной проблемы представляется создание специализированных порталов для малых и средних компаний в целях хранения их баз данных, на которых будет осуществляться централизованная защита информации. При этом компании, оказывающие услуги по обеспечению информационной безопасности, будут защищать облачное пространство, в котором представители малого и среднего бизнеса разместят свои информационные системы персональных данных или воспользуются системами, предоставляемыми интегратором. Указанные порталы должны быть созданы на уровне муниципальных образований не только для бизнеса, но и для муниципальных организаций, или на уровне региона для нескольких муниципалитетов одновременно [4]. Деятельность указанных порталов должна быть урегулирована на уровне региона путем принятия соответствующего законодательного акта субъекта России и быть аналогичной созданным бизнес-инкубаторам и другим массовым программам поддержки малого и среднего бизнеса.

Разработка и внедрение таких порталов должны осуществляться в рамках общегосударственных программ, например федерального проекта «Информационная безопасность» программы

[1] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ. URL: http://pravo.gov.ru (дата обращения: 11.03.2024).

[2] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: проект Федерального закона № 502104-8 (ред., принятая ГД ФС РФ в I чтении 23.01.2024). URL: https://sozd.duma.gov.ru/ (по состоянию на 23.01.2024).

[3] Бойко А., Кинякина Е. Малый бизнес попросил депутатов смягчить законопроект об оборотных штрафах. URL: https://www.vedomosti.ru/economics/articles/2024/03/22/1027194-malii-biznes-poprosil-deputatov-smyagchit-zakonoproekt-ob-oborotnih-shtrafah (дата обращения: 23.03.2024).

«Цифровая экономика Российской Федерации»[1] [11]. Это позволит привлечь для создания облачного пространства крупные федеральные компании и федеральное финансирование.

Только в этом случае корректные действия по наведению порядка в области защиты персональных данных не приведут к массовому банкротству компаний, оказывающих услуги или продающих товары населению. Принятие же проекта Федерального закона № 502104-8 в его современном виде приведет к возвращению России в сфере электронной торговли на 5 – 10 лет назад и переходу на торговлю товарами в магазинах. При этом невведение предлагаемой ответственности крайне негативно скажется на состоянии защиты персональных данных в Российской Федерации.

Обсуждение и заключение

Подводя итог проведенному анализу, мы сделали следующие выводы. С одной стороны, отмена исключений, ранее установленных пунктами 1-6 части 2 статьи 22 ФЗ «О персональных данных», значительно увеличила количество организаций, которые должны уведомлять Роскомнадзор об обработке персональных данных. В целом это привело к улучшению ситуации с соблюдением законодательства о персональных данных, но внесенные изменения привели к значительной нехватке специалистов. Требуются не только обучение тысяч технических сотрудников, которые обеспечивают защиту информации в информационных системах, но и подготовка десятков тысяч нетехнических сотрудников, осуществляющих работу с физическими лицами по сбору, обработке и последующему использованию их персональных данных.

Второй вывод связан с введенной системой информирования об инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных. Для организаций, которые владеют объектами критической информационной инфраструктуры или эксплуатируют их, указанное информирование не должно представлять существенных трудностей. Но для организаций, которые ранее даже не информировали Роскомнадзор о том, что они обрабатывают персональных данные, обеспечить полноценную защиту информационных систем представляется трудноразрешимой задачей, поскольку осуществлять защиту от кибератак, выявлять и расследовать киберинциденты малые и средние компании, а также муниципальные организации, самостоятельно не способны, должны быть созданы соответствующие технические и организационные возможности, позволяющие им это делать. Для этого на уровне регионов и в центральных аппаратах министерств должны быть созданы облачные пространства, предназначенные для защиты информационных систем персональных данных от кибератак. Кроме этого, в субъектах Российской Федерации должна быть разработана правовая база для коллективной защиты персональных данных с участием государства. Недопустимо оставлять малые и средние организации, как в коммерческой, так и в государственной сфере, один на один со всем западным сообществом, осуществляющим кибератаки на российскую инфраструктуру фактически на промышленной основе. При этом вступление в силу норм административной ответственности для малых и средних компаний, индивидуальных предпринимателей и муниципальных организаций необходимо отложить не менее чем на год.

СПИСОК ИСТОЧНИКОВ

1. Основы информационной безопасности в МЧС России / Р.Ш. Хабибулин, А.Н. Прокопенко, П.Н. Жукова и др. Москва: Академия ГПС МЧС России, 2023. 649 с.
2. Прокопенко А.Н., Жукова П.Н., Страхов А.А. Актуальные киберугрозы в Российской Федерации на современном этапе и перспективы обеспечения информационной безопасности // Материалы 32 международной научно-технической конференции «Системы безопасности 2023». Москва: Академия ГПС МЧС России, 2023. С. 69 – 76.
3. Новые горизонты развития системы информационного права в условиях цифровой трансформации: монография / отв. ред.: Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. Москва: Институт государства и права РАН, 2022. 368 с.

[1] План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации»: утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 № 2). URL: http://static.government.ru по состоянию на 09.01.2018. Письмо Минцифры России от 13.10.2021 № П25-18390-ОГ «О рассмотрении обращения» (вместе с «Паспортом федерального проекта «Информационная безопасность»). СПС «КонсультантПлюс».

4. Трансформация информационного права: монография / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. Москва: Институт государства и права РАН, 2023. 256 с.
5. Кривоухов А.А. Проблема безопасности персональных данных на цифровых платформах // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей IX Всероссийской научно-практической конференции. 2022. С. 86-91.
6. Рябинин В. Обработка персональных данных: обновленные требования // Учреждения здравоохранения: бухгалтерский учет и налогообложение. 2022. № 10. С. 26 – 35.
7. Данилов С. Защита персональных данных: новые требования и обязанности фирм // Практическая бухгалтерия. 2022. № 10. С. 69 – 75.
8. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (постатейный) // Пешкова (Белогорцева) Х.В., Прокопенко А.Н., Ротко С.В., Рыдченко К.Д., Солдаткина О.Л., Струков К.В., Тимошенко Д.А. Специально для системы ГАРАНТ, 2021 г.
9. Правовое регулирование оборота персональных данных в условиях современных вызовов и угроз: монография / Минбалеев А.В., Добробаба М.Б., Ефремов А.А. и др. Саратов: Амирит, 2023. 138 с.
10. Амелин Р.В., Колоколов А.В., Колоколова М.Д., Липатов Э.Г., Свечникова И.В., Чаннов С.Е. Постатейный комментарий к Кодексу РФ об административных правонарушениях. Часть первая: комментарий к главам 1 – 14 КоАП РФ (под общ. ред. Л.В. Чистяковой). Москва: ИД «ГроссМедиа»: РОСБУХ, 2019. 2672 с.
11. Право цифровой среды: монография / под ред. Т.П. Подшивалова, Е.В. Титовой, Е.А. Громовой. Москва: Проспект, 2022. 896 с.

REFERENCES

1. Osnovy informacionnoj bezopasnosti v MCHS Rossii: uchebnik / R.SH. Habibulin, A.N. Prokopenko, P.N. ZHukova i dr. Moskva: Akademiya GPS MCHS Rossii, 2023. 649 s.
2. Prokopenko A.N., ZHukova P.N., Strahov A.A. Aktual'nye kiberugrozy v Rossijskoj Federacii na sovremennom etape i perspektivy obespecheniya informacionnoj bezopasnosti // Materialy 32 mezhdunarodnoj nauchno-tekhnicheskoj konferencii «Sistemy bezopasnosti 2023». Moskva: Akademiya GPS MCHS Rossii, 2023. S. 69 – 76.
3. Novye gorizonty razvitiya sistemy informacionnogo prava v usloviyah cifrovoj transformacii: monografiya / otv. red.: T.A. Polyakova, A.V. Minbaleev, V.B. Naumov. Moskva: Institut gosudarstva i prava RAN, 2022. 368 s.
4. Transformaciya informacionnogo prava: monografiya / otv. red. T.A. Polyakova, A.V. Minbaleev, V.B. Naumov. Moskva: Institut gosudarstva i prava RAN, 2023. 256 s.
5. Krivouhov A.A. Problema bezopasnosti personal'nyh dannyh na cifrovyh platformah // Problemy informacionnogo obespecheniya deyatel'nosti pravoohranitel'nyh organov: sbornik statej IX Vserossijskoj nauchno-prakticheskoj konferencii. 2022. S. 86-91.
6. Ryabinin V. Obrabotka personal'nyh dannyh: obnovlennye trebovaniya // Uchrezhdeniya zdravoohraneniya: buhgalterskij uchet i nalogooblozhenie. 2022. № 10. S. 26 - 35.
7. Danilov S. Zashchita personal'nyh dannyh: novye trebovaniya i obyazannosti firm // Prakticheskaya buhgalteriya. 2022. № 10. S. C. 69 - 75.
8. Kommentarij k Federal'nomu zakonu ot 27 iyulya 2006 g. № 152-FZ «O personal'nyh dannyh» (postatejnyj) // Peshkova (Belogorceva) H.V., Prokopenko A.N., Rotko S.V., Rydchenko K.D., Soldatkina O.L., Strukov K.V., Timoshenko D.A. Special for GARANT 2021.
9. Pravovoe regulirovanie oborota personal'nyh dannyh v usloviyah sovremennyh vyzovov i ugroz: monografiya / Minbaleev A.V., Dobrobaba M.B., Efremov A.A. i dr. Saratov: OOO «Amirit». 2023. 138 s.
10. Amelin R.V., Kolokolov A.V., Kolokolova M.D., Lipatov E.G., Svechnikova I.V., CHannov S.E. Postatejnyj kommentarij k Kodeksu RF ob administrativnyh pravonarusheniyah. CHast' pervaya: kommentarij k glavam 1 – 14 KoAP RF (pod obshch. red. L.V. CHistyakovoj). ID «GrossMedia»: ROSBUH, 2019. 2672 s.
11. Pravo cifrovoj sredy: monografiya / pod red. T.P. Podshivalova, E.V. Titovoj, E.A. Gromovoj. Prospekt, 2022. 896 s.

Информация об авторе:
Прокопенко Алексей Николаевич, кандидат технических наук, доцент, профессор кафедры информационных технологий (в составе учебно-научного комплекса автоматизированных систем и информационных технологий) Академии Государственной противопожарной службы МЧС России, Alex_prokop@rambler.ru, ORCID: 0000-0002-4455-086X, РИНЦ SPIN-код: 4527-0898, РИНЦ Author ID: 692625.
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Prokopenko Alexey N., Candidate in Technical Sciences (Research doctorate), Associate Professor, Professor of the Department of Information Technologies (as part of the Educational and Scientific Complex of Automated Systems and Information Technologies) of the Academy of the State Fire Fighting Service of the Ministry of Emergency Situations of Russia, Alex_prokop@rambler.ru, ORCID: 0000-0002-4455-086X, RINC SPIN code: 4527-0898, RINC Author ID: 692625.
The author has read and approved the final version of the manuscript.

Статья получена: 05.04.2024.
Статья принята к публикации: 25.06.2024.
Статья опубликована онлайн: 28.06.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.