В.В. Бухарин

*А*КТУАЛЬНЫЕ АСПЕКТЫ ЗАКОНОТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ УКРЕПЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ COVID-19

Пандемия COVID-19 оказала серьезное влияние на экономику и социальные отношения во многих странах. Столкнувшись с новыми вызовами и угрозами в данный период, Россия, как и другие страны, была вынуждена обратить пристальное внимание на решение проблем информационной безопасности. В статье представлен анализ основных изменений в российском законодательстве в области информационной безопасности в период пандемии, рассматривается широкий спектр документов стратегического и техническое характера, посвященных вопросам криптографии и электронной подписи, персональным данным, национальной платежной системе, банковской безопасности и др. В проведенном исследовании показано, что в связи с ростом количества угроз в информационной сфере необходимо дальнейшее совершенствование законодательства, его доработка, прежде всего, в области импортозамещения в IT сфере, сбора и хранения персональных и биометрических данных, дистанционного предоставления услуг и идентификации пользователя и др. С управленческой точки зрения, в условиях высшей степени развития эпидемического процесса работа осуществлялась в основном на управленческом и техническом уровнях. Начало проведения СВО потребовало в большей степени принятия решений на уровне институциональном, используя законодательную основу и методы, применяемые в предшествующий период.

Ключевые слова: информационная безопасность, информационный суверенитет, национальная безопасность, ипортозамещение, пандемия, COVID-19, кибератаки, информационные технологии, ИТ, цифровой суверенитет, киберугрозы.

The COVID-19 pandemic has had a major impact on the economy and social relations in many countries. Faced with new challenges and threats in this period, Russia, like other countries, was forced to pay close attention to solving information security problems. This article is devoted to the

* *Владислав Викторович Бухарин* — к.и.н., доцент факультета государственного управления МГУ имени М.В. Ломоносова, Москва, Россия; *e-mail:* Bukharin@spa.msu.ru

analysis of the main changes in Russian legislation in the field of information security during the pandemic. The author analyzed a wide range of documents of a strategic and technical nature on issues such as cryptography and electronic signatures, personal data, the national payment system, banking security, etc. According to the author, due to the growing number of threats in the information sphere, it is necessary to further improve legislation, improvement, primarily in the field of import substitution in the IT field, collection and storage of personal and biometric data, remote provision of services and user identification, etc. From a managerial point of view, in the conditions of the highest degree of development of the epidemic process, work was carried out mainly at the managerial and technical levels. The launch of the Special Military Operation required more decision-making at the institutional level, using the legislative framework and methods used in the previous period.

Key words: information security, information sovereignty, national security, import substitution, pandemic, COVID-19, cyber-attacks, information technology, IT, digital sovereignty, cyber threats.

COVID-19 впервые был зафиксирован в китайском городе Ухань в декабре 2019 г. К весне 1920 г. вирус охватил почти весь мир, вызвав, по утверждению Всемирной организации здравоохранения (ВОЗ), пандемию. По данным университета Джонса Хопкинса, за ноябрь 2021 г. в мире от болезни скончалось около 5,5 млн чел.[1] Подобная ситуация потребовала от правительств всех стран введения жестких ограничительных мер и ускоренной цифровизации экономики[2]. Удаленная работа, онлайн-обучение и широкий спектр дистанционных услуг[3] стали новой реальностью для многих государств, в том числе и для Российской Федерации.

Произошедшие изменения не только обострили традиционные угрозы в сфере информационных технологий (IT), но и вывели проблему информационной безопасности на новый уровень. Данными факторами, а также степенью изучения проблемы обусловлена новизна исследования. Анализ законотворческой деятельности РФ в области укрепления информационной безопасности в условиях COVID-19 представляется актуальным,

[1] COVID-19 Map // Johns Hopkins Coronavirus Resource Center/ [Электронный ресурс]. URL: https://coronavirus.jhu.edu/map.html (дата обращения: 06.01.2022).

[2] *Прохоров А., Коник Л.* Цифровая трансформация. Анализ, тренды, мировой опыт. Издание второе, исправленное и дополненное. М.: ООО «КомНьюс Груп», 2019.

[3] *Днепровская Н.В., Шевцова И.В.* Открытые образовательные ресурсы и цифровая среда обучения // Высшее образование в России. 2020. №12. С. 144–155.

поскольку изменения, произошедшие в законодательстве, стали не только основой дальнейшего совершенствования законодательного регулирования, но и защитой от аналогичных угроз в целях обеспечения информационного суверенитета в период проведения специальной военной операции (СВО). В условиях информационной войны, геополитического противостояния России и так называемого коллективного Запада, проблема информационной безопасности стала одной из приоритетных задач государства. Однако законотворческая деятельность РФ в области укрепления информационной безопасности до настоящего времени не стала предметом комплексного изучения. Отдельным вопросам развития информационного права были посвящены работы Т.А. Поляковой, А.В. Минбалеевой, Н.В. Кототковой, Е.В. Виноградовой, Г.Э. Адыгезаловой, С.Д. Гринько, Е.И. Гончарова, Т.В. Шатковской[4]. Уголовно-правовая проблематика нашла отражение в работах Р.Р. Карданова, А.А. Шапошникова, Ю.В. Гульбинского[5]. Проблемы информационной безопасности рассматривались в работах О.М. Хохловой, А.К. Рожковой, А.В. Хохловой, В.В. Бухарина, А.К. Дубеня, В.Н. Шельменкова, Г.О. Крылова, А.П. Курило, С.Л. Ларионовой[6]. Вопросам цифрового государственного

[4] *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Формирование системы информационного права как научного направления: этапы развития и перспективы // Государство и право. 2019. № 2. С. 80–92; *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75–87; Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / под общ. ред. Т.А. Поляковой. Саратов: Амирит. 2020; *Виноградова Е.В., Полякова Т.А.* О месте информационного суверенитета в конституционно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. № 1 (63). С. 32–49; *Адыгезалова Г.Э.* Динамизм российского права в условиях пандемии // Теория и практика общественного развития. 2020. № 5 (147). С. 77–81; *Гринько С.Д.* Противодействие посягательствам на информационную безопасность // Право и государство: теория и практика. 2020. № 3 (183). С. 246–249; *Гончаров Е.И., Шатковская Т.В.* Проблемы применения цифровой подписи в электронном документообороте России // Северо-Кавказский юридический вестник. 2020. № 2. С. 97–103.

[5] *Карданов Р.Р.* Уголовно-правовая охрана информационной безопасности // Вестн. Сибирского юридического института МВД России. 2022. № 2 (47). С. 58–63; *Шапошников А.А., Гульбинский Ю.В.* Уголовно-правовой анализ публичного распространения ложной информации о новой коронавирусной инфекции (COVID-19) // Уголовная юстиция. 2022. № 19. С. 29–32.

[6] *Дубень А.К.* Аспекты и угрозы информационной безопасности в эпоху современных информационных войн // Вестн. Удмуртского университета. Сер. «Экономика и право». 2022. № 6. С. 1064–1068; *Хохлова О.М., Рожкова А.К., Хохлова А.В.* Информационная безопасность в системе национальной безопасности

управления, а также перспективным технологическим решениям, связанным с переходом от цифровых к нейрокоммуникационным технологиям в сфере государственного управления были посвящены работы Г.Л. Купряшина, А.Е. Шрамма, Косорукова А.А.[7] и др. Целью данной статьи является анализ эволюции законодательной базы Российской Федерации в IT сфере в условиях пандемии. Хронологические рамки работы охватывают период с декабря 2019 г. по 24 февраля 2022 г. Нижняя граница исследования связана с началом эпидемии. Верхней хронологической границей послужили: спад эпидемии и начало СВО. Несмотря на то, что в настоящее время ВОЗ официально не отменил пандемию, 1 июля 2022 г. Роспотребнадзор, в связи со снижением интенсивности эпидемического процесса, снял введенные в стране ограничения[8]. На фоне геополитических изменений, произошедших в феврале 2022 г., влияние фактора COVID-19 на информационную безопасность представляется менее значимым, поскольку на первый план вышли задачи военного характера, многие из которых непосредственно связаны с ведением боевых операций. В соответствии с поставленной целью исследования, автор попытался решить следующие задачи: определить основные угрозы в IT сфере, проанализировать законы, принятые в РФ в период пандемии в области информационной безопасности, выявить основные направления деятельности государственных институтов для дальнейшего совершенствования законодательного регулирования IT сферы. В качестве методологической основы

современного российского общества // Инновационное развитие науки: фундаментальные и прикладные проблемы. Монография. Петрозаводск: МЦНП «Новая наука», 2021; *Бухарин В.В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестн. МГИМО-Университета. 2016. № 6 (51). С. 76–91; *Шельменков В.Н.* Информационная безопасность в дистанционном банковском обслуживании // Труды Института государства и права РАН. 2020. № 3. С. 188–204; *Крылов Г.О., Курило А.П., Ларионова С.Л.* Вопросы информационной безопасности национальной платежной системы России // Инновации и инвестиции. 2016. № 8. С. 140–147.

[7] *Купряшин Г.Л., Шрамм А.Е.* О перспективах третьей волны парадигмы цифрового государственного управления // Государственное управление. Электронный вестник. 2021. № 84. С. 256–276. URL: http://e-journal.spa.msu.ru/uploads/vestnik/2021/vipusk__84._fevral_2021_g./strategija_zifrovoi_ ekonomiki/kupryashin_schramm.pdf (дата обращения: 02.02.2023); *Косоруков А.А.* Перспективные технологические решения в сфере построения нейроцифрового государственного управления // Социодинамика. 2021. № 6. С. 53–66.

[8] Роспотребнадзор снимает введенные из-за пандемии ограничения // Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека [Электронный ресурс]. URL: https://www.rospotrebnadzor.ru/about/info/news/news_details.php?ELEMENT_ID=22056 (дата обращения: 02.02.2023).

исследования были использованы принципы историзма и объективности, которые реализованы при анализе угроз, возникших в сфере IT в связи с COVID-19. В соответствии с принципом объективности был изучен широкий круг источников нормативно-правового характера, не получивших освещения в отечественных и зарубежных исследованиях. При сопоставлении различных редакций законов, формулировок и определений, в анализе наиболее значимых стратегических документов автор использовал компаративный метод исследования.

В докладе Интерпола, озаглавленном «Глобальный ландшафт киберугрозы COVID-19» отмечалось, что киберпреступники атакуют «компьютерные сети и системы отдельных лиц, предприятий и даже глобальных организаций, в то время как киберзащита может быть снижена из-за смещения акцента в связи с кризисом в области здравоохранения»[9]. В качестве основных угроз периода эпидемии COVID-19 в данном докладе выделены вредоносные домены и программное обеспечение, программы-вымогатели. Авторы доклада сообщали о существовании тысяч сайтов, содержавших информацию о COVID-19, часть из которых была создана злоумышленниками и использовалась для распространения спама или вредоносных программ, а также фишинга[10]. Вредоносные, шпионские и троянские программы, по заявлению Интерпола, были обнаружены в интерактивных картах коронавируса и веб-сайтах. Больницы, медицинские центры и государственные учреждения, утверждалось в докладе, часто становились мишенью киберпреступников. Медицинские учреждения особенно были подвержены атакам вымогателей, поскольку большой объем работы не позволял их IT-отделам оперативно блокировать медицинские системы. Противодействие угрозам, обозначенным в докладе, безусловно, имеет приоритетное значение. Вместе с тем стоит отметить, что информационная безопасность значительно шире кибербезопасности[11] и соответственно спектр угроз может быть дополнен согласно перечню, приведенному профессором МГТУ имени Н.Э. Баумана

---

[9] Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception // INTERPOL [Электронный ресурс]. URL: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (дата обращения: 02.02.2023).

[10] От англ. fishing «рыбная ловля, выуживание», тип киберпреступления, при котором преступники выдают себя за надежный источник в сети Интернет.

[11] *Abassi R., Ben Chehida Douss A.* Cybersecurity Crisis Management and Lessons Learned From the COVID-19 Pandemic. USA: IGI Global. 2022; *Okereafor K.* Cybersecurity in the COVID-19 Pandemic. US, UK: CRC Press. 2021.

Алексеем Марковым[12], а также информацией, опубликованной в блоге Касперского[13]. Среди наиболее значимых угроз, отмеченных экспертами, следует отметить атаки с использованием социальной инженерии, угрозы кибербезопасности в домашнем офисе, угрозы бесперебойной работы, уязвимости каналов связи и инструментов для совместной работы. Ряд экспертов, в числе наиболее значимых, отмечали следующие проблемы: сбор данных о физиологическом состоянии граждан в связи с распространением вируса и вопросы защиты персональных данных, адаптация к цифровому формату трудовой деятельности и дистанционное обучение, обострение противоборства в информационной сфере[14]. Спектр угроз достаточно велик[15]. Анализ каждой из перечисленных заслуживает отдельного исследования, однако представляется более важным изучение действий РФ в ответ на вызовы COVID-19.

В первую очередь, необходимо рассмотреть вопросы нормативно-правового характера[16]. Существует мнение, что информационная сфера Россия не была готова к тем вызовам, с которыми она столкнулась в период COVID-19. Однако, в юридическом плане незадолго до эпидемии был принят ряд достаточно важных документов, в том числе и стратегического характера. Так, невозможно обойти вниманием «Концепцию создания и функционирования национальной системы управления данными, утвержденную распоряжением Правительства Российской Федерации от 3 июня 2019 г. № 1189-р»[17]. Основной целью концепции, как сказано в самом до-

---

[12] *Марков А.* Информационная безопасность в условиях пандемии COVID-19 // Российский совет по международным делам [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasnost-v-usloviyakh-pandemii-covid-19/ (дата обращения: 02.02.2023).

[13] Kaspersky Team. Год красного локдауна — как COVID-19 повлиял на кибербезопасность // Блог Касперского [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/pandemic-year-in-infosec/30316/ (дата обращения: 02.02.2023).

[14] *Горач Н.Н., Филатова И.В.* Вызовы и угрозы информационной безопасности преступлениями, совершаемыми в условиях пандемии COVID-19 // Вестн. Московского университета МВД России. 2020. № 8. С. 102–105.

[15] *Дубень А.К.* Указ. соч.; *Хохлова О.М., Рожкова А.К., Хохлова А.В.* Указ. соч.

[16] Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5 С. 75–87; Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / под общ. ред. Т.А. Поляковой. Саратов: Амирит, 2020; Виноградова Е.В., Полякова Т.А. Указ. соч.; Адыгезалова Г.Э. Указ. соч.; Гринько С.Д. Указ. соч.

[17] Утверждена Концепция создания и функционирования национальной системы управления данными // Правительство России [Электронный ресурс]. URL: http://government.ru/docs/36940/ (дата обращения: 02.02.2023).

кументе, является реализация мероприятий федерального проекта «Цифровое государственное управление»[18] национальной программы «Цифровая экономика Российской Федерации»[19]. Создание национальной системы управления данными (НСУД), согласно тексту концепции, должно способствовать «повышению эффективности создания, сбора и использования государственных данных как для предоставления государственных и муниципальных услуг и осуществления государственных и муниципальных функций, так и для обеспечения потребности физических и юридических лиц в доступе к информации»[20]. На первом этапе формирования системы планировалось провести эксперимент с 1 июля 2019 г. по 31 марта 2020 г. по апробации основных подходов к формированию данной системы при активном участии различных министерств, банков и страховых организаций. Согласно заявлению премьер-министра Д.А. Медведева (2012–2020), прозвучавшему в 2019 г., национальная система управления данными в полном объеме будет функционировать в 2022 г.[21]. Он также отметил, что подобная система «не предполагает» объединение всех баз данных в одну глобальную, а речь идет лишь об их взаимодействии. В мае 2021 г. произошла доработка концепции: были добавлены новые термины и определения, четко определены элементы НСУД, проведена гармонизация, систематизация и исправление, ликвидация противоречий[22].

---

[18] «Цифровое государственное управление» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/ activity/directions/882/ (дата обращения: 06.01.2022).

[19] «Цифровая экономика РФ» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 06.01. 2022).

[20] Распоряжение Правительства РФ от 03.06.2019 N 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 годы» // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/554802572 (дата обращения: 02.02.2023).

[21] *Пятигорская А.* Национальная система управления данными заработает в 2022 году // «Парламентская газета» [Электронный ресурс]. URL: https://www.pnp.ru/economics/nacionalnaya-sistema-upravleniya-dannymi-zarabotaet-v-2022-godu.html (дата обращения: 02.02.2023).

[22] *Ключевская Н.* Минэкономразвития России подготовило новые поправки в части формирования национальной системы управления данными // Портал ГАРАНТ.РУ. URL: http://www.garant.ru/news/1461761/ (дата обращения: 02.02.2023).

Еще одним важным стратегическим документом стал президентский указ № 490 о развитии искусственного интеллекта (ИИ) от 10.10.2019. Документ содержал в себе блок национальной стратегии в данной области. Предполагаемый срок реализации стратегии был рассчитан на период до 2030 г.[23] Необходимо отметить, что процесс создания стратегии изначально занял достаточно продолжительное время. Начало работы по формулированию концептуальных основ часто связывается с одним из выступлений В.В. Путина, прозвучавших в 2017 г. Однако непосредственная разработка подходов к формированию национальной стратегии началась только в 2019 г., когда президентом был утвержден перечень непосредственных поручений. Сложно переоценить значение разработок в области ИИ[24], которые, безусловно, необходимы для Российской Федерации. Детальное изучение указа позволяет сделать вывод, что авторы руководствовались в первую очередь экономическими соображениями. Учитывая, что в разработке стратегии активное участие принимал «Сбербанк», предположение об экономической детерминанте дальнейшего развития искусственного интеллекта в России представляется вполне обоснованным, что вызывает некоторые опасения. Необходимо подчеркнуть, что в документе недостаточно детально прописаны приоритетные цели и задачи, которые планируется решать с помощью искусственного интеллекта, а также его использование для решения проблем промышленности и бизнеса, науки и образования, здравоохранения. Среди положительных аспектов данной стратегии стоит отметить, что, согласно документу, предполагается финансирование прикладных и научных исследований в области ИИ, разработки отечественного программного и аппаратного обеспечения, например, отечественных высокоскоростных и энергоэффективных процессоров. Само по себе это может стать важным шагом на пути достижения так называемого цифрового суверенитета[25].

Наиболее значимым стратегическим документом, принятым за последние несколько лет, стала стратегия национальной без-

---

[23] Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201910110003 (дата обращения: 02.02.2023).

[24] *Шумский С.* Искусственный интеллект: вызовы и угрозы России // Российский совет по международным делам [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/ analytics/iskusstvennyy-intellekt-vyzovy-i-ugrozy-rossii/ (дата обращения: 02.02.2023).

[25] *Бухарин В.В.* Указ. соч.

опасности РФ, утвержденная в 2021 г.[26] Информационная безопасность впервые вошла в перечень стратегических национальных приоритетов. Угрозы информационной безопасности были зафиксированы и в стратегии 2015 г.[27], однако в новой редакции данной проблеме был посвящен отдельный раздел. Среди нововведений следует отметить, что в документе говорится о целях, роли и влиянии транснациональных корпораций в IT-сфере, их стремлении монополизировать Интернет, установить контроль СИМ, ввести цензуру, блокировать неподконтрольные им интернет-платформы. Политика транснациональных корпораций не имеет законодательных оснований, противоречит нормам международного права. Руководствуясь политическими причинами, пользователям интернета «навязывается искаженный взгляд на исторические факты, а также на события, происходящие в РФ и в мире»[28]. Важным представляется, что «целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве»[29].

В апреле 2021 г. были утверждены основы государственной политики РФ в сфере международной информационной безопасности[30]. Несмотря на значительные изменения, произошедшие в мировой политике и международных отношениях, данный документ стал в определенной степени плановым обновлением аналогичного стратегического документа № Пр-1753[31] (рассчитанного на период до 2020 г.), утвержденного президентом в 2013 г. В до-

---

[26] Указ Президента Российской Федерации от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации» // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/media/files/file/l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf (дата обращения: 02.02.2023).

[27] Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201512310038 (дата обращения: 02.02.2023).

[28] Указ Президента Российской Федерации от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации» // Указ. соч.

[29] Там же.

[30] Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202104120050 (дата обращения: 02.02.2023).

[31] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. (утв. Президентом РФ 24.07.2013 N Пр-1753) // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/ (дата обращения: 02.02.2023).

кументе содержались новые формулировки определений «международная информационная безопасность» и «система обеспечения международной информационной безопасности». Обновленные формулировки представляются более удачными. В 2013 г. под международной информационной безопасностью понимались международные и национальные институты, обязанные «регулировать» деятельность «субъектов глобального информационного пространства»[32]. Однако наличие регулирующих функций не означает их позитивное использование в целях предотвращения, ликвидации или минимизации угроз информационной безопасности[33]. Таким образом, корректировка определения представляется вполне обоснованной. В новом документе был расширен перечень угроз в области информационной безопасности, детализированы основные направления реализации государственной политики в данной области, а также сделан акцент на соблюдении общепризнанных принципов и норм международного права и проблемах равноправного партнерства.

Федеральный закон об информации, информационных технологиях и о защите информации[34] был принят еще в 2006 г. За прошедшие 16 лет в него были внесены десятки изменений. Среди поправок, принятых в период пандемии COVID-19, стоит отметить изменения, касающиеся регулирования деятельности социальных сетей, например, ответственности за распространение недостоверной информации и о порядке ограничения доступа к недостоверной информации[35].

В период 1920–1921 гг. в сфере информационной безопасности решались не только стратегические задачи. Достаточно большая работа была проделана в области стандартизации, процедур оценки соответствия средств защиты информации, мероприятий по аттестации объектов информатизации согласно требованиям безопасности информации. Был принят или доработан ряд документов,

---

[32] Там же.

[33] Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Там же.

[34] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.02.2023).

[35] Федеральный закон от 01.07.2021 N 260-ФЗ «О внесении изменения в Федеральный закон “Об информации, информационных технологиях и о защите информации”» // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_388902/ (дата обращения: 02.02.2023).

направленных на решение технических вопросов. Например, министерством цифрового развития, связи и массовых коммуникаций был утвержден новый классификатор отечественного программного обеспечения[36]. Данный документ значительно отличался от его предварительной версии, опубликованной ранее. Новый классификатор состоял из 11 разделов и 111 классов. Учитывая, что в реестре программного обеспечения в 2020 г. насчитывалось более 7 тыс. наименований, доработка классификатора с целью упрощения поиска продуктов заказчиками, а также с учетом импортозамещения «сквозных» технологий, была необходима. Важно отметить, что работа над классификатором была продолжена и в 2022 г.: в конце года в классификатор стало возможным добавлять программное обеспечение, предназначенное для виртуальной и дополненной реальности. Кроме того, в качестве примера можно провести новую редакцию постановления правительства РФ о продукции, подлежащей обязательной сертификации или «декларации о соответствии»[37] и некоторые другие нормативные документы.

Необходимость организации удаленной работы в период пандемии ускорила внедрение электронного документооборота и электронной подписи. Был решен ряд юридических проблем, препятствующих, по мнению экспертов, практическому применению данных технологий[38]. Так, например, были определены основные требования к простой электронной подписи, которая используется для дачи согласия на обработку персональных данных[39]. Значи-

---

[36] Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22.09.2020 N 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» (Зарегистрировано в Минюсте России 29.10.2020 N 60646) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/7362/ (дата обращения: 02.02.2023).

[37] Постановление Правительства Российской Федерации от 01.12.2009 N 982 (ред. от 04.07.2020) «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии» // Правительство России [Электронный ресурс]. URL: http://government.ru/docs/all/70507/ (дата обращения: 02.02.2023).

[38] Гончаров Е.И., Шатковская Т.В. Указ. соч.

[39] Постановление Правительства РФ от 15.10.2021 N 1754 «Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации" подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202110180013 (дата обращения: 02.02.2023).

тельные изменения произошли в законодательстве о квалифицированной электронной подписи. Реформирование системы выдачи квалифицированной электронной подписи началось в конце декабря 2019 г. «Федеральный закон "О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» от 27.12.2019 № 476-ФЗ (последняя редакция)"»[40] уточнил понятие «аккредитованный удостоверяющий центр», а также повысил требования к удостоверяющим центрам. Стоит отметить, что проблема фальсификации электронной подписи к середине 2019 г. перешла из теоретической плоскости в практическую. Согласно заявлению Росреестра, в мае 2019 г. был зафиксирован первый случай похищения квартиры с помощью поддельной электронной подписи[41]. Потерпевшему удалось отстоять свои права[42], однако данный случай дал повод для обсуждения вопроса о введении государственной монополии на выдачу электронных подписей. В конце 2020 г. был утвержден перечень угроз безопасности, связанных с электронной подписью[43]. С 1 июля 2021 г. Федеральная

[40] Федеральный закон «О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" от 27.12.2019 N 476-ФЗ (последняя редакция)» // Федеральная налоговая служба [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/10071944/ (дата обращения: 02.02.2023).

[41] *Рассохин А.* Электронная подпись оставила без квартиры // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3969174 (дата обращения: 02.02.2023).

[42] Информация по делу № 02-3237/2019 // Официальный портал судов общей юрисдикции города Москвы [Электронный ресурс]. URL: https://mosgorsud.ru/rs/babushkinskij/services/cases/civil/details/ 7ae9082f-aeec-49b9-9822-2bd1eae932e0?participants=%D1%81%D0%B0%D0%BB%D1%82%D0%BE%D0%B2%D1%81%D0%BA%D0%B8%D0%B9 (дата обращения: 02.02.2023).

[43] Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 26 ноября 2020 г. N 624 «Об утверждении перечня угроз безопасности, актуальных при идентификации заявителя — физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре» (Зарегистрировано в Минюсте России 22.12.2020 N 61689) // Электронный

налоговая служба России (ФНС) начала выдачу квалифицированных электронных подписей, наряду с коммерческими удостоверяющими центрами, которые оказывали данную услугу на платной основе. Стоит отметить, что центры, не прошедшие аккредитацию согласно обновленным требованиям 63-ФЗ, лишилась права выдачи электронной подписи. Количество сертифицированных центров значительно сократилось. С 1 января 2022 г. право выдачи квалифицированной электронной подписи руководителям организаций и индивидуальным предпринимателям полностью перешло к ФНС и ее доверенным лицам[44]. Предполагалось, что подобная система будет функционировать в переходный период до начала 2023 г. Сотрудники компаний были обязаны с 1 января 2023 г. использовать квалифицированную подпись физлица (выдается в аккредитованных центрах), а также электронную доверенность, удостоверяющую их право подписи документов от имени организации.

Широкое распространение электронного документооборота и электронной подписи тесно связано с проблемой использования сертифицированных, согласно требованиям Федеральной службы безопасности Российской Федерации (ФСБ), криптографических средств. Внедрение отечественных алгоритмов шифрования было начато в 90-е гг. Одним из первых отечественных алгоритмов цифровой эпохи стал ГОСТ 28147-89[45]. На смену устаревшим стандартам[46] за последние годы были введены ГОСТ 34.12-2018[47] и ГОСТ

фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/573161169 (дата обращения: 02.02.2023).

[44] В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» с 01.01.2022 обязанность по выпуску квалифицированной электронной подписи возлагается на Федеральную налоговую службу (пункты выдачи КЭП) // Федеральная налоговая служба [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/ucfns/ (дата обращения: 02.02.2023).

[45] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования от 02 июня 1989 // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200007350 (дата обращения: 02.02.2023).

[46] Извещение о порядке использования алгоритма блочного шифрования ГОСТ 28147-89 // Федеральная служба безопасности Российской Федерации [Электронный ресурс]. URL: http://www.fsb.ru/fsb/science/single.htm%21id%3D10438446%40fsbResearchart.html (дата обращения: 02.02.2023).

[47] ГОСТ 34.12-2018. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Блочные шифры // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200161708 (дата обращения: 02.02.2023).

34.13.2018[48]. С 15 июля 2020 г. по 1 марта 2020 г. был реализован пилотный проект по использованию российских систем шифрования в государственных органах[49]. Цель эксперимента состояла в подготовке к полному переходу на отечественное программное обеспечение госорганов, организаций и граждан. О результатах пилотного проекта не сообщалось, однако Министерство цифрового развития, связи и массовых коммуникаций России «предложило расширить свои полномочия в части установки требований к отечественной криптографии, применяемой госорганами»[50]. В 2020 г. в области применения криптографической защиты банковской сферы был утвержден ряд документов, определивших требования: «к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы…»[51]; «к техническим средствам и программному обеспечению», реализующим СКЗИ в платежных устройствах с терминальным ядром»[52];

---

[48] ГОСТ 34.13-2018. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200161709 (дата обращения: 02.02.2023).

[49] Постановление Правительства Российской Федерации от 30.06.2020 № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202007030010 (дата обращения: 02.02.2023).

[50] *Аскерова Т.* Минцифры установит требования к криптографии для госорганов // «Парламентская газета» [Электронный ресурс]. URL: https://www.pnp.ru/politics/mincifry-ustanovit-trebovaniya-k-kriptografii-dlya-gosorganov.html (дата обращения: 02.02.2023).

[51] «Требования к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. N 382-П» (утв. ФСБ России 24.01.2020, 28.02.2020 N ФТ-56-3/32) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104752/FT_32.pdf (дата обращения: 02.02.2023).

[52] «Функционально-технические требования к техническим средствам и программному обеспечению, реализующим СКЗИ в платежных устройствах с терминальным ядром» (утв. Банком России 28.02.2020 N ФТ-56-3/33) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104753/FT_33.pdf (дата обращения: 02.02.2023).

к платежным картам[53]; аппаратному модулю безопасности[54] и др. Банк России при участии ФСБ России, кредитных организаций, субъектов национальной платежной системы активно работал над внедрением российских криптографических алгоритмов в рамках развития значимых платежных систем и обеспечения их информационной безопасности и киберустойчивости[55].

В период пандемии банки расширили дистанционное обслуживание населения. Детальный анализ документов позволяет сделать вывод о том, что отдельные вопросы требуют более детальной проработки. Например, юридически не закреплено понятие дистанционного банковского обслуживания, недостаточно основательно проработан вопрос дистанционной идентификации пользователей[56].

В стране был предпринят ряд шагов по укреплению информационной безопасности национальной платежной системы[57], среди которых следует отметить Положение Банка России № 719-П от 04.06.2020, посвященное проблеме защиты информации при осуществлении денежных переводов[58]. Данный документ пришел на смену аналогичному «Положению № 382-П»[59], действовавшему до

---

[53] «Функционально-технические требования к платежным картам (криптомодуль, приложение)» (утв. Банком России 28.02.2020 N ФТ-56-3/34) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104754/FT_34.pdf (дата обращения: 02.02.2023).

[54] «Функционально-технические требования к аппаратному модулю безопасности (HSM-модуль)» (утв. Банком России 28.02.2020 N ФТ-56-3/35) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104755/FT_35.pdf (дата обращения: 02.02.2023).

[55] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 гг. // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/ File/83253/onrib_2021.pdf (дата обращения: 02.02.2023).

[56] *Шельменков В.Н.* Указ. соч. С. 201.

[57] *Крылов Г.О., Курило А.П., Ларионова С.Л.* Указ. соч.

[58] Положение Банка России от 04.06.2020 N 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (Зарегистрировано в Минюсте России 23.09.2020 N 59991) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Queries/UniDbQuery/File/90134/1119 (дата обращения: 02.02.2023).

[59] Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» // Портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/70091962/ (дата обращения: 02.02.2023).

1 января 2022 г. Новое положение достаточно сильно отличается от предыдущего. Модификации подверглись как общая структура документа, так и его отдельные разделы. Можно выделить наиболее существенные изменения: расширение перечня организаций, на которые распространялось действие положения; добавление предписания об обязательном соответствии Стандарту ГОСТ Р 57580.1-2017[60] для всех субъектов системы; установление жестких требований к банковским платежных агентам и субагентам; наложение обязательств по сертификации прикладного программного обеспечения автоматизированных систем и приложений на операторов по переводу денежных средств, согласно правилам безопасности, не ниже 5 уровня доверия, а для значимых и системно значимых кредитных организаций — не ниже 4 уровня; ужесточение требований по защите персональных данных и использования электронной подписи.

В период пандемии значительные изменения произошли в законодательстве о персональных данных. Количество документов, регламентирующих данную область, достаточно велико и требует отдельного исследования. За последние годы произошло ужесточение требований к работе с персональными данными. Например, в Федеральный закон от 27.07.2006 № 152-ФЗ в период пандемии были внесены изменения от 27.12.2019 № 480-ФЗ, от 24.04.2020 № 123-ФЗ, от 08.12.2020 № 429-ФЗ, от 30.12.2020 № 515-ФЗ, от 30.12.2020 № 519-ФЗ, от 11.06.2021 № 170-ФЗ, от 02.07.2021 № 331-ФЗ[61]. Среди наиболее значимых из них стоит отметить добавление статьи 10 (Федеральный закон от 30.12.2020 № 519-ФЗ), регламентирующей «особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения». Важным представляется, что теперь оператор обязан оформить отдельное от прочих документов соглашение на обработку персональных данных; предоставить человеку право выбора, какими именно данными он хочет делиться (не заключать соглашений на полный доступ ко всей информации, как это было ранее); «молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку пер-

[60] ГОСТ Р 57580.1-2017 // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс]. URL: http://protect.gost.ru/document1.aspx?control=31&id=218176 (дата обращения: 02.02.2023).

[61] Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/? docbody&nd=102108261 (дата обращения: 02.02.2023).

сональных данных, разрешенных субъектом персональных данных для распространения»[62]; ранее выданное разрешение можно отозвать у любого оператора, обрабатывающего персональные данные (кроме «обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления функций, полномочий и обязанностей»[63]).

Еще одним важным изменением 152-ФЗ стало дополнение его статьёй № 23 (Федеральный закон от 11.06.2021 № 170-ФЗ), озаглавленной «Федеральный государственный контроль (надзор) за обработкой персональных данных». В статье подчеркивалось, что контроль за соблюдением требований по обработки персональных данных осуществляется федеральным органом власти[64].

Ответственность за нарушения в работе с персональными данными была ужесточена в период пандемии. Согласно ФЗ от 24.02.2021 № 19-ФЗ[65] впервые с 2017 г. был существенно увеличен размер штрафов. С 27 марта 2021 г. за любые правонарушения в области персональных данных предполагается штраф, а не предупреждение. За повторные нарушения были установлены более высокие суммы штрафов. Срок давности привлечения к административной ответственности по правонарушениям в области персональных данных был увеличен с трех месяцев до одного года.

Решение проблем информационной безопасности потребовало совершенствования уголовно-правовых норм. Например, были введены различные степени наказания за распространение ложной информации об инфекции COVID-19[66].

Стоит отметить, что не все законодательные инициативы последних лет можно оценить однозначно положительно. Обширной критике подвергся предложенный Министерством экономического развития законопроект «О внесении изменений в статью 53 Федерального закона "О связи"»[67]. В пояснительной записке к данно-

---

[62] Там же.

[63] Там же.

[64] Там же.

[65] Федеральный закон от 24.02.2021 № 19-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/ 0001202102240010 (дата обращения: 02.02.2023).

[66] *Карданов Р.Р.* Указ. соч.; *Шапошников А.А., Гульбинский Ю.В.* Указ. соч.

[67] О внесении изменений в статью 53 Федерального закона «О связи» // Федеральный портал проектов нормативных правовых актов [Электронный ресурс].

му проекту говорилось о том, что необходимо дать возможность операторам «передавать сведения об абонентах и оказываемых им услугах третьим лицам при наличии согласия абонента»[68]. Под «сведениями» авторы законопроекта имели ввиду «базы данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента»[69]. Подобные предложения подверглись жесткой критике со стороны вице-спикера Госдумы, члена фракции «Единая Россия» П.О. Толстого. В своем телеграм-канале депутат написал: «Идея поставить на поток оборот персональных данных не просто сомнительная, а откровенно вредительская. Возможно, мы что-то пропустили: разве банки и операторы связи уже настолько обезопасили информацию о своих клиентах и решили вопрос с мошенниками, что теперь можно торговать ею?»[70].

Ускоренная цифровизация экономики требует наличия кадров с «уникальными» компетенциями. Согласно приказу[71] Министерства труда и социальной защиты Российской Федерации в 2021 г., был утвержден профессиональный стандарт «Специалист по моделированию, сбору и анализу данных цифрового следа»[72]. Несмотря на тот факт, что документ вступил в силу в марте 2022 г., можно говорить о появлении новой профессии.

В ходе исследования был сделан вывод, что среди основных угроз кибербезопасности в период пандемии оказались проблемы, связанные с распространением вредоносного программного обеспечения и программ вымогателей, с фишингом и кибератаками в адрес госучреждений и частных лиц, атаками с использованием

URL: https://regulation.gov.ru/projects/ List/AdvancedSearch#departments=6&npa=122564 (дата обращения: 02.02.2023).

[68] Пояснительная записка к проекту федерального закона «О внесении изменений в статью 53 Федерального закона «О связи» // Федеральный портал проектов нормативных правовых актов [Электронный ресурс]. URL: https://regulation.gov.ru/Files/GetFile?fileid=cc05f573-3e64-4d16-a7d4-6c399345bf71 (дата обращения: 02.02.2023).

[69] Там же.

[70] *Петр Толстой* // Официальный канал Telegram Петра Толстого [Электронный ресурс]. URL: https://t.me/petr_tolstoy/1174 (дата обращения: 06.01.2022).

[71] Приказ Министерства труда и социальной защиты Российской Федерации от 09.07.2021 № 462н «Об утверждении профессионального стандарта "Специалист по моделированию, сбору и анализу данных цифрового следа" (Зарегистрировано в Минюсте России 30.07.2021 N 64502)» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202108020014 (дата обращения: 02.02.2023).

[72] What is your Digital Footprint? // The University of Aberdeen [Электронный ресурс]. URL: https://www.abdn.ac.uk/toolkit/documents/uploads/infosec-campaign-digifootprint.pdf (дата обращения: 02.02.2023).

социальной инженерии, а также с незаконным сбором биометрических данных и информации о физиологическом состоянии граждан и д.р. Премьер-министр РФ М.В. Мишустин в своем выступлении на форуме «Digital Almaty 2023» отметил, что COVID-19 «подстегнул цифровизацию и активное использование людьми всех возможных сервисов», Россия вошла в десятку стран с «наиболее высоким уровнем использования информационных технологий в государственном секторе»[73]. Проведенный анализ документов позволяет сделать вывод, что за последние несколько лет на законодательном уровне проделана огромная работа в области укрепления информационной безопасности Российской федерации, ликвидации или уменьшения выявленных угроз. В рассматриваемый период были приняты как стратегические документы, так и целые серии законодательных актов, связанных с банковской безопасностью, криптографией и электронной подписью, персональными данными и др. Однако некоторые решения принимались в экстренном порядке, фрагментарно, не всегда имели системный характер. Отдельные инициативы были направлены в первую очередь на решение экономических вопросов, в то время как проблемы национальной безопасности и национального суверенитета в IT-сфере отодвигались на второй план. Постоянное возрастание количества угроз требует совершенствования законодательства, его дальнейшей доработки, прежде всего, в области импортозамещения в IT-сфере, сбора и хранения персональных и биометрических данных, дистанционного предоставления услуг и идентификации пользователя и др. С управленческой точки зрения, следует отметить, что в условиях высшей степени развития эпидемического процесса работа осуществлялась в основном на управленческом и техническом уровнях. Начало проведения СВО потребовало в большей степени принятия решений на уровне институциональном, используя законодательную основу и методы, применяемые в предшествующий период.

Литература

Адыгезалова Г.Э. Динамизм российского права в условиях пандемии // Теория и практика общественного развития. 2020. № 5 (147). С. 77–81.

Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестн. МГИМО-Университета. 2016. № 6 (51). С. 76–91.

[73] Михаил Мишустин принял участие в работе международного цифрового форума «Digital Almaty 2023» // Правительство России [Электронный ресурс]. URL: http://government.ru/news/47680/ (дата обращения: 03.02.2023).

Виноградова Е.В., Полякова Т.А. О месте информационного суверенитета в конституционно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. № 1 (63). С. 32–49.

Гончаров Е.И., Шатковская Т.В. Проблемы применения цифровой подписи в электронном документообороте России // Северо-Кавказский юридический вестн. 2020. № 2. С. 97–103.

Горач Н.Н., Филатова И.В. Вызовы и угрозы информационной безопасности преступлениями, совершаемыми в условиях пандемии COVID-19 // Вестн. Московского университета МВД России. 2020. № 8. С. 102–105.

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования от 02 июня 1989 // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200007350

ГОСТ 34.12-2018. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Блочные шифры // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200161708

ГОСТ Р 57580.1-2017 // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс]. URL: http://protect.gost.ru/document1.aspx?control=31&id=218176

Гринько С.Д. Противодействие посягательствам на информационную безопасность // Право и государство: теория и практика. 2020. № 3 (183). С. 246–249.

Днепровская Н.В., Шевцова И.В. Открытые образовательные ресурсы и цифровая среда обучения // Высшее образование в России. 2020. № 12. С. 144–155.

Дубень А.К. Аспекты и угрозы информационной безопасности в эпоху современных информационных войн // Вестн. Удмуртского университета. Сер. «Экономика и право». 2022. № 6. С. 1064–1068.

Карданов Р.Р. Уголовно-правовая охрана информационной безопасности // Вестн. Сибирского юридического института МВД России. 2022. № 2 (47). С. 58–63.

Косоруков А.А. Перспективные технологические решения в сфере построения нейроцифрового государственного управления // Социодинамика. 2021. № 6. С. 53–66.

Крылов Г.О., Курило А.П., Ларионова С.Л. Вопросы информационной безопасности национальной платежной системы России // Инновации и инвестиции. 2016. № 8. С. 140–147.

Купряшин Г.Л., Шрамм А.Е. О перспективах третьей волны парадигмы цифрового государственного управления // Государственное управление. Электронный вестник. 2021. № 84. С. 256–276. URL: http://e-journal.spa.msu.ru/

uploads/vestnik/2021/ vipusk__84._fevral_2021_g./strategija_zifrovoi_ekonomiki/kupryashin_schramm.pdf

Марков А. Информационная безопасность в условиях пандемии COVID-19 // Российский совет по международным делам [Электронный ресурс]. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasn ost-v-usloviyakh-pandemii-covid-19/

Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе / под общ. ред. Т.А. Поляковой. Саратов: Амирит, 2020.

О внесении изменений в статью 53 Федерального закона «О связи» // Федеральный портал проектов нормативных правовых актов [Электронный ресурс]. URL: https://regulation.gov.ru/projects/List/AdvancedSearch#departments=6&npa=122564

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 N Пр-1753) // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/

Положение Банка России от 04.06.2020 N 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (Зарегистрировано в Минюсте России 23.09.2020 N 59991) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Queries/UniDbQuery/File/90134/1119

Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» // Портал ГАРАНТ.РУ. URL: https://www.garant.ru/products/ipo/prime/doc/70091962/

Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. № 5. С. 75–87.

Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Формирование системы информационного права как научного направления: этапы развития и перспективы // Государство и право. 2019. № 2. С. 80–92.

Постановление Правительства Российской Федерации от 01.12.2009 N 982 (ред. от 04.07.2020) «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии» // Правительство России [Электронный ресурс]. URL: http://government.ru/docs/all/70507/

Постановление Правительства Российской Федерации от 30.06.2020 № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202007030010

Постановление Правительства РФ от 15.10.2021 N 1754 «Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации" подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202110180013

Пояснительная записка к проекту федерального закона «О внесении изменений в статью 53 Федерального закона «О связи» // Федеральный портал проектов нормативных правовых актов [Электронный ресурс]. URL: https://regulation.gov.ru/Files/GetFile?fileid=cc05f573-3e64-4d16-a7d4-6c399345bf71

Приказ Министерства труда и социальной защиты Российской Федерации от 09.07.2021 № 462н «Об утверждении профессионального стандарта "Специалист по моделированию, сбору и анализу данных цифрового следа" (Зарегистрировано в Минюсте России 30.07.2021 N 64502)» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/ 0001202108020014

Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22.09.2020 № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» (Зарегистрировано в Минюсте России 29.10.2020 N 60646) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/7362/

Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 26 ноября 2020 г. № 624 «Об утверждении перечня угроз безопасности, актуальных при идентификации заявителя — физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре» (Зарегистрировано в Минюсте России 22.12.2020 N 61689) // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/573161169

Прохоров А., Коник Л. Цифровая трансформация. Анализ, тренды, мировой опыт. Издание второе, исправленное и дополненное. М.: ООО «КомНьюс Груп», 2019.

Распоряжение Правительства РФ от 03.06.2019 N 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 гг.» // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/554802572

«Требования к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. N 382-П» (утв. ФСБ России 24.01.2020, 28.02.2020 № ФТ-56-3/32) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/ Document/File/104752/FT_32.pdf

Указ Президента Российской Федерации от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации» // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/media/files/file/ l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf

Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/ 0001202104120050

Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/ Document/View/0001201512310038

Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/ Document/View/0001201910110003

Утверждена Концепция создания и функционирования национальной системы управления данными // Правительство России [Электронный ресурс]. URL: http://government.ru/docs/36940/

Федеральный закон «О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" от 27.12.2019 № 476-ФЗ (последняя редакция)» // Федеральная налоговая служба

[Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/10071944/

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ. // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 01.07.2021 N 260-ФЗ «О внесении изменения в Федеральный закон "Об информации, информационных технологиях и о защите информации"» // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant. ru/document/cons_doc_LAW_388902/

Федеральный закон от 24.02.2021 № 19-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication. pravo.gov.ru/Document/View/0001202102240010

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261

«Функционально-технические требования к аппаратному модулю безопасности (HSM-модуль)» (утв. Банком России 28.02.2020 N ФТ-56-3/35) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104755/FT_35.pdf

«Функционально-технические требования к платежным картам (криптомодуль, приложение)» (утв. Банком России 28.02.2020 N ФТ-56-3/34) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104754/FT_34.pdf

«Функционально-технические требования к техническим средствам и программному обеспечению, реализующим СКЗИ в платежных устройствах с терминальным ядром» (утв. Банком России 28.02.2020 N ФТ-56-3/33) // Банк России [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/104753/FT_33.pdf

Хохлова О.М., Рожкова А.К., Хохлова А.В. Информационная безопасность в системе национальной безопасности современного российского общества // Инновационное развитие науки: фундаментальные и прикладные проблемы: монография. Петрозаводск: МЦНП «Новая наука». 2021.

Шапошников А.А., Гульбинский Ю.В. Уголовно-правовой анализ публичного распространения ложной информации о новой коронавирусной инфекции (COVID-19) // Уголовная юстиция. 2022. № 19. С. 29–32.

Шельменков В.Н. Информационная безопасность в дистанционном банковском обслуживании // Труды Института государства и права РАН. 2020. № 3. С. 188–204.

Abassi R., Ben Chehida Douss A. Cybersecurity Crisis Management and Lessons Learned From the COVID-19 Pandemic. USA: IGI Global. 2022.

Okereafor K. Cybersecurity in the COVID-19 Pandemic. US, UK: CRC Press. 2021.

Статья поступила в редакцию 21.01.2023