

DOI: 10.17803/1729-5920.2024.206.1.133-143

А. А. Уваров

Всероссийский государственный университет юстиции
(РПА Минюста России)
г. Москва, Российская Федерация

Информационная безопасность граждан России: современное состояние

Резюме. В статье рассматриваются концептуальные, отраслевые и практические аспекты правового регулирования информационной безопасности граждан России. В связи с развитием информационных технологий, ростом цифровых информационных ресурсов, их транснациональной природой усложняется контроль за безопасностью использования этих ресурсов в интересах граждан. Внедрение новых информационных технологий представляет определенные технические трудности для неподготовленных к ним граждан и вызывает в связи с этим некоторую социально-психологическую напряженность. Развитие законодательства об информационной безопасности тесно связано с конституционным принципом свободы массовой информации, который предусматривает некоторые ограничения этой свободы в интересах безопасности в различных сферах нашей жизни. Специфика современных информационных технологий требует качественно нового подхода и самостоятельного направления деятельности государства для обеспечения безопасности как граждан, так и самого государства и общества в целом. Отмечается, что помимо злонамеренных информационных вбросов недружественных государств существуют и собственные проблемы, связанные с низким уровнем цифровой культуры граждан, проблемы гарантированности сохранения тайны данных цифрового документооборота и др. Проблемными участками правового регулирования в области информационной безопасности граждан остается: практика сокрытия необходимой для реализации прав граждан информации органами публичной власти под грифом служебной тайны; недостоверная и недобросовестная реклама; распространение информационной продукции, представляющей опасность для здоровья и нормального развития детей, и т.д. Обращается внимание на особенности предоставления информационных ресурсов в условиях чрезвычайного и военного положения. Отмечается высокая востребованность Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», благодаря которому удалось ранжировать субъекты и объекты информационной инфраструктуры в зависимости от их сферы реализации и целей безопасности.

Ключевые слова: коммуникационные технологии; угрозы информационной безопасности; вредоносный контент; безопасность граждан; цифровая культура; информационные ограничения; цифровые данные; защита информации; информационная гарантированность; информационные объекты; субъекты информационных ресурсов

Для цитирования: Уваров А. А. Информационная безопасность граждан России: современное состояние. *Lex russica*. 2024. Т. 77. № 1. С. 133–143. DOI: 10.17803/1729-5920.2024.206.1.133-143

Information Security as to Russian Citizens: Current State

Alexander A. Uvarov

The All-Russian State University of Justice
Moscow, Russian Federation

Abstract. The paper examines the conceptual, sectoral and practical aspects of the legal regulation of information security as to Russian citizens. Due to the development of information technologies, the growth of digital information resources, and their transnational nature, it is becoming more difficult to control the safety of using

© Уваров А. А., 2024

these resources in the interests of citizens. The introduction of new information technologies presents certain technical difficulties for citizens who are unprepared for them and causes some socio-psychological tension in this regard. The development of legislation on information security is closely linked to the constitutional principle of freedom of the media, which provides for some restrictions on this freedom in the interests of security in various spheres of our lives. The specifics of modern information technologies require a qualitatively new approach and an independent direction of the state's activities to ensure the safety of both citizens and the state itself and society as a whole. It is noted that in addition to malicious information stuffing by unfriendly states, there are also their own problems associated with the low level of digital culture of citizens, problems of guaranteeing the secrecy of digital document management data, etc. Problematic areas of legal regulation in the field of information security as to citizens remain: the practice of concealing information necessary for the realization of citizens' rights by public authorities classified as secret; unreliable and unfair advertising; distribution of information products that pose a danger to the health and normal development of children, etc. Attention is drawn to the specifics of the provision of information resources in conditions of emergency and martial law. There is a high demand for Federal Law No. 187-FZ dated 07.26.2017 «On the Security of the Critical Information Infrastructure of the Russian Federation», which made it possible to rank subjects and objects of information infrastructure depending on their scope of implementation and security objectives.

Keywords: communication technologies; threats to information security; malicious content; security of citizens; digital culture; information restrictions; digital data; information security; information safety; objects of information; subjects of information resources

Cite as: Uvarov AA. Information Security as to Russian Citizens: Current State *Lex russica*. 2024;77(1):133-143. (In Russ.). DOI: 10.17803/1729-5920.2024.206.1.133-143

Информационные ресурсы всё более становятся не только фактором развития и процветания нашего общества, залогом полного, гарантированного и всестороннего обеспечения российских граждан основными правами и свободами, но и фактором его стабильности и безопасности. Важность проблемы информационной безопасности многократно возросла с бурным развитием информационных и коммуникационных технологий. Данная проблема превратилась в неотъемлемую составляющую национальной безопасности, связанную с угрозами вмешательства во внутренние дела российского государства и защитой его граждан от вредоносного информационно-психологического воздействия¹.

Актуальность проблемы информационной безопасности также связана с увеличением

количества компьютерных атак на российские информационные ресурсы, активизацией деятельности иностранных разведывательных служб, распространением недостоверной информации и др. При этом анонимность использования в электронно-цифровой среде информационных ресурсов облегчает совершение многих опасных преступлений (финансирование терроризма, легализация преступных доходов, распространение наркотиков и психотропных веществ и др.). На информационные угрозы и задачи по их предотвращению указывается в целом ряде федеральных государственных документов².

Особую актуальность приобрели вопросы информационной безопасности в связи с международным военным конфликтом на Украине. Еще до его начала в отдельных федеральных

¹ См.: Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утв. Указом Президента РФ от 09.05.2017 № 203 ; Стратегия национальной безопасности Российской Федерации, утв. Указом Президента РФ от 02.07.2021 № 400 // URL: pravo.gov.ru (дата обращения: 01.10.2023).

² См.: Доктрина информационной безопасности, утв. Указом Президента РФ от 05.12.2016 № 646 ; Стратегия противодействия экстремизму в Российской Федерации до 2025 года, утв. Указом Президента РФ от 09.11.2022 № 809 (необходимость проведения мониторинга массовой информации для запрета распространения экстремистской идеологии, создания информационных банков данных экстремистских материалов (пп. «д» п. 32)) ; Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, утв. Указом Президента РФ от 09.11.2022 № 809 (предупреждение с целью предотвращения угроз информационных вбросов деструктивной идеологии (саморазрушение общества), внедрение антиобщественных стереотипов поведения, причинение вреда нравственному здоровью людей, усиление социально-культурного расслоения, подрыв доверия к

документах³ уже обозначались основные угрозы этой безопасности: подрыв государственного суверенитета; террористические, экстремистские и иные преступные цели; проведение через электронные сети атак на информационные ресурсы государства; использование технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий и др. В настоящее время по указанным основаниям признаны экстремистскими и запрещены на территории РФ такие крупнейшие зарубежные цифровые платформы, как: Google Meta, Facebook, Twitter, Instagram, TikTok, YouTube.

По мнению А. А. Ганеева, «...недружественное давление на целостность, конфиденциальность и доступность информационных массивов кратно увеличивается и приобретает всё более агрессивные формы, остро ощущается недостаточность мер для обеспечения безопасности персональных данных граждан и сотрудников предприятий, защита значимых объектов критической информационной инфраструктуры, коммерческой тайны, управления активами информационной безопасности»⁴.

Необходимо признать, что объективно и сам по себе факт развития информационно-коммуникативных технологий уже вызывает некоторую социально-психологическую напряженность в обществе. Так, согласно проведенным в Курской области опросам, респонденты отмечают, что вследствие внедрения информационно-телекоммуникационных технологий жизнедеятельность в современном обществе становится опаснее или скорее опаснее (так считают 17,6 и

40,1 % соответственно). Для 38,3 % опрошенных жителей региона идет нарастание ощущения незащищенности в информационно-коммуникационной среде.

Чаще всего граждане сталкиваются со спамом, т.е. рассылкой корреспонденции лицам, не выразившим желание ее получать, — 86,1 %. На втором месте по частоте встречаемости находятся вирусы, ведущие к блокированию браузера или компьютера, — 78,7 %. И наконец, на третьем и четвертом месте находится фишинг (попытка несанкционированного доступа к логинам и паролям) и его частная версия — взлом и воровство в социальных сетях (соответственно 40,7 и 47,3 %) ⁵.

По статистическим данным количество компьютерных атак на частных лиц в 2022 г. в России увеличилось на 44 %. В этом же году произошло не менее 60 крупных утечек персональных данных, содержащих более 230 млн записей с личной информацией граждан⁶. Надо отметить, что преобладают здесь киберпреступления в финансовой среде, чья доля начиная с 2016 г. по стране ежегодно составляет 98 %, потерпевшими по которым выступают клиенты банковских организаций и сами банки⁷.

Тенденции развития российского законодательства об информационной безопасности граждан связаны с их защищаемыми законодательством интересами. Конституционный принцип свободы массовой информации (ч. 4 и 5 ст. 29 Конституции РФ) на самом деле имеет пределы своего распространения, касающиеся не только названного в ч. 4 перечня сведений государственной тайны. В упомянутых выше доктринальных документах уже отмечались

институтам государства и др. (п. 17)) ; Стратегия государственной национальной политики Российской Федерации на период до 2025 года, утв. Указом Президента РФ от 19.12.2012 № 1666 (необходимость формирования в обществе обстановки нетерпимости к пропаганде и распространению идей экстремизма, ксенофобии, национальной исключительности (пп. «в» п. 21), обеспечение открытости и публичности рассмотрения ситуаций, связанных с конфликтами в сфере межнациональных (межэтнических) отношений (пп. «з» п. 21)) // URL: pravo.gov.ru (дата обращения: 01.10.2023).

³ См.: Основы государственной политики России в области международной информационной безопасности, утв. Указом Президента РФ от 12.04.2021 № 213 // URL: pravo.gov.ru (дата обращения: 01.10.2023).

⁴ Ганеев А. А. Кибербезопасность в условиях агрессивной внешней информационной среды // Сборник материалов международного форума / под общ. ред. Р. Н. Минниханова. Казань, 2022. С. 286.

⁵ Кривоухов А. А. К оценке уровня безопасности личности в информационно-коммуникационной среде со стороны криминала // Мир науки. Социология, филология, культурология. 2020. № 1. Т. 11 С. 4.

⁶ Капранов О. Эксперты по информационной безопасности назвали главные угрозы на 2023 год // URL: <https://rg.ru/2023/01/17-god.html> (дата обращения: 02.10.2023).

⁷ Афанасьева В. Р. Проблемы и пути решения информационной безопасности в банковской сфере // Эволюция российского права : материалы XVII Международной научной конференции, Уральский государственный университет. Екатеринбург, 2019. С. 395–397.

некоторые виды информационных ресурсов, общественные носители которых, в соответствии с ч. 5 ст. 13 Конституции РФ, подлежат запрету, поскольку их деятельность по распространению этих информационных ресурсов угрожает государственной, общественной и личной безопасности граждан. Эти запреты обусловлены политическим режимом демократического государства. Разумеется, в авторитарном или тоталитарном государстве перечень запретов информационной свободы может быть значительно расширен за счет запретов на информацию, которая каким-либо образом несовместима с обязательной официальной государственной идеологией, с религиозными догматами клерикального государства или с установками военного диктаторского режима.

Конституционные ограничения права на информацию, предусмотренные частью 3 ст. 17 и частью 3 ст. 55 Конституции РФ, направлены на запрет распространения следующих видов информации:

1) разжигающей национальную ненависть и рознь;

2) фальсифицированной и нарушающей нормы приличия и нравственности;

3) посягающей на честь и достоинство граждан, представляющей опасность и вред физическому и духовно-нравственному состоянию людей;

4) искажающей память о прошлом, историю страны, посягающей на отечественные ценности поколений;

5) инициирующей разрушительные процессы (техногенные, природные, социальные).

Как в любом демократическом государстве, в России существуют и специальные ограничители информации — это разного рода запрещенная для посторонних лиц информация. Ограни-

ченность распространения такой информации может быть продиктована интересами государственной безопасности⁸, бизнеса⁹, органов публичной власти¹⁰. Действующим законодательством закреплён целый ряд прав граждан на охрану их личной информации (врачебная тайна, тайна исповеди, тайна усыновления, журналистская тайна, банковская тайна, депутатская тайна, тайна персональных данных и др.). Вопрос о закрытости (тайне) информации непосредственно связан с интересами граждан даже тогда, когда информация не является личной. Так, сохранение государственной тайны необходимо для обеспечения защиты государственного суверенитета нашего государства, а значит, всего общества и каждого гражданина. Сохранение коммерческой тайны, возможно, не так очевидно для обеспечения интересов каждого отдельного гражданина, но с учетом действия рыночных законов эта норма обеспечивает бизнесу благоприятные условия для конкуренции в производстве товаров и услуг, а значит, дает возможность более полного и качественного удовлетворения потребностей граждан.

Обилие информационных ресурсов и переход с бумажной на интернет-платформу делает этот ресурс с учетом международного характера последней недостаточно управляемым и контролируемым с точки зрения необходимости минимизации его негативного воздействия на защищаемые внутренним законодательством государственные, общественные и личные интересы граждан.

По мнению Т. Я. Хабриевой, «как самостоятельное новое направление государственной деятельности признается обеспечение безопасности личности, общества и государства при применении информационных технологий, оборота цифровых данных»¹¹. Вместе с тем,

⁸ Федеральный закон от 21.07.1993 № 5465-1-ФЗ «О государственной тайне» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

⁹ Федеральный закон от 29.07.2004 № 94-ФЗ «О коммерческой тайне» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

¹⁰ Федеральный закон от 26.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»; Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

Данные законы, к сожалению, не содержат положений о так называемой служебной тайне, поэтому законодатель здесь пошел по пути «обратного» регулирования, т.е. установил обязанность органов публичной власти обеспечить гарантированную доступность установленных этими законами информационных ресурсов их деятельности.

¹¹ Хабриева Т. Я. Доклад на Петербургском международном юридическом форуме «Конституционный контроль: развиваем доктрину и совершенствуем практику» // Российская юстиция. 2023. № 6. С. 3–8.

как отмечает Т. Е. Колосова, «существующий сейчас уровень защиты цифровых данных не позволяет полностью отказаться от бумажного документооборота по следующим причинам: 1) легкость тиражирования и фальсификации электронных данных; 2) как программная, так и материальная составляющая электронных хранилищ информации на данный момент не обладают необходимым уровнем долговечности и надежности (так физические носители цифровой информации крайне не долговечны и редко служат дольше 10–15 лет, в то время как программы обработки и хранения информации обновляются еще быстрее).

Что же касается “облачных” технологий, то они далеко не совершенны. А с учетом складывающейся в последние годы геополитической обстановки следует учитывать, что подавляющее большинство дата-центров, обеспечивающих хранение таких данных, расположены за пределами нашей страны, а в случае неблагоприятного развития международной обстановки это может привести к полной утрате доступа к ним российских обладателей и пользователей, хранящейся в них информации»¹².

Следует отметить, что цифровая трансформация сама по себе продуцирует появление новых возможностей реализации интересов и потребностей человека, а вместе с ними возникновение новых прав человека и гражданина как участника всемирного информационного пространства. Традиционными и привычными стали права человека на доступ и использование коммуникационных сетей Интернета, право на защиту от компьютерных атак и действий хакеров, право на создание своих собственных компьютерных программ и иных компьютерных произведений. Цифровизация охватила целые отрасли индустрии, стала неотъемлемым фактором государственного управления и предоставления государственных услуг.

С точки зрения интересов личности данный процесс цифровизации, с одной стороны, на-

целен на обеспечение ее удобства, поскольку позволяет быстро получить необходимую для этого информацию, автоматизировав трудоемкий процесс поиска такой информации и выполнения иных рутинных операций. С другой стороны, как отмечает А. А. Подупейко, «повсеместное появление камер, развитие специального программного обеспечения... позволяет контролировать информацию о личности. При этом личность спокойно существует во множестве этих электронных баз данных, не задумываясь о том, что практически утрачивает право на личную жизнь, право на безопасность»¹³.

Расширяются и сами объекты информационных ресурсов. Так, помимо традиционной вербальной информации, с помощью современных технологий возникают возможности передачи на расстояние не только изображений, но и запахов, а также тактильных ощущений. По мнению отдельных авторов, термины «информационная безопасность» и «информационная приватность» стали использовать вместе. В научно-практической литературе приводятся примеры «негативного прогресса», совершенствования цифровых технологий в деле криминализации в области нарушений отдельных прав человека. Как отмечает А. Геращенко, «если в аналоговом мире злоумышленник мог получить (не только из сети Интернет) копию паспорта субъекта и оформить на него микрозайм, то сегодня утечка, к примеру, изображения гражданина (или геометрии его лица) может закончиться созданием злоумышленниками его дипфейка и использованием его личности в своих интересах, например для трудоустройства в качестве дистанционного работника»¹⁴. В настоящее время в международном праве определено три сферы наиболее активного применения методов биометрических данных: пограничный контроль, банковские онлайн-операции и сфера обслуживания клиентов¹⁵.

Одним из наиболее серьезных факторов риска в сфере информационной безопасности

¹² Колосова Т. Е. Проблемы реализации охранительной функции государства в сфере защиты прав человека в цифровом пространстве // Актуальные проблемы государства и права. 2022. Т. 6. № 2. С. 155.

¹³ Подупейко А. А. Некоторые вопросы обеспечения конституционных прав и свобод личности в условиях цифровой трансформации // Актуальные проблемы достижения целей устойчивого развития в условиях цифровой трансформации государства и права в Республике Беларусь : материалы республиканской науч.-практ. конференции. Минск, 2022. С. 316–317.

¹⁴ Геращенко А. Диалектика приватности в условиях развития информационной безопасности // Международное правосудие. 2022. № 4. С. 69.

¹⁵ Международная конвенция о защите физических лиц при автоматизированной обработке персональных данных : заключена в Страсбурге 28 января 1980 г. // СЗ РФ. 2014. № 5.

граждан, по мнению М. В. Пономарева, является неприемлемо низким уровень развития их цифровой культуры¹⁶. На доктринальном уровне уже сформулирован тезис о том, что государство должно обеспечить защищенность граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности¹⁷. Свое развитие данный тезис нашел в более поздних документах Правительства РФ, где отмечается, что для предотвращения угроз информационной безопасности граждан необходимо с раннего возраста прививать знания по распознаванию фишинговых сайтов и писем, телефонного мошенничества, созданию надежных паролей, распознаванию недостоверной информации и другого вредоносного контента.

Основными же принципами этой деятельности являются: усиление ответственности государства в информационной сфере наряду с консолидацией организационных структур гражданского общества по активизации усилий в проведении информационных компаний и иных мероприятий, формирование у граждан ответственного отношения к личной информационной безопасности в цифровом пространстве¹⁸. В апреле 2020 г. внесены изменения в административный и уголовный кодекс, предусматривающие ответственность «за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан».

На практике бывает достаточно сложно выявить истинные мотивы и цели человека, рас-

пространяющего такую информацию. Порой в подобной ситуации мы имеем дело с людьми, которые либо искренне убеждены в достоверности такой информации, либо легкомысленно полагают, что это всего лишь их «безобидная шутка», в действительности не представляя масштабы и последствия ее распространения. В этой связи Г. П. Корнев предлагает различать дезинформацию и заблуждение: «Если корреспондент сознательно ставит перед собой задачу ввести реципиента в заблуждение, то информационный процесс приобретает дезинформационную интенцию. Когда корреспондент при передаче ложных сведений уверен в их истинности, имеет место заблуждение»¹⁹.

Тем не менее гражданам, которые получают вредоносный контент в результате таких заблуждений, от этого не легче, поэтому и авторам, и издателям необходимо тщательно проверять такую информацию на достоверность, а для тех, кто в погоне за сенсацией все-таки пренебрегает этим советом, надо также предусмотреть соответствующую юридическую ответственность (за небрежность, халатность и т.п.).

Правовые основы информационной безопасности граждан — это не только конституционные нормы и доктрины, но и отраслевые нормативные правовые акты, а также постановления высших судов России, в которых более предметно отражены вопросы этой безопасности, наряду с общими вопросами политики предоставления потребителям публичной информации²⁰. Разумеется, в каждом отраслевом институте имеются и свои специфические

¹⁶ Пономарев М. В. Цифровая компетенция граждан как фактор информационной безопасности современного мегаполиса // Правовые аспекты безопасности города Москвы: исторический опыт, актуальные тенденции и перспективы : материалы круглого стола, проведенного в рамках XVI Фестиваля науки города Москвы. М., 2022. С. 113–119.

¹⁷ Пп. «д» п. 27 Доктрины информационной безопасности, утв. Указом Президента РФ от 05.12.2016 № 646 // URL: pravo.gov.ru (дата обращения: 01.10.2023).

¹⁸ См.: Концепция формирования и развития культуры информационной безопасности граждан РФ утв. распоряжением Правительства РФ от 22.12.2022 № 4088-р // URL: pravo.gov.ru (дата обращения: 01.10.2023).

¹⁹ Корнев Г. П. Дезинформация и заблуждение в информационном пространстве // Труды III Всероссийской научной конференции. М., 2021. С. 210–214.

²⁰ Федеральный закон от 13.01.1995 № 6-ФЗ «О средствах массовой информации» ; Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ; Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» ; Федеральный закон от 13.02.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» ; постановление Правительства РФ от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти» ; постановление Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения

проблемы информационной безопасности. Так, проблемным участком в области защиты прав потребителей оказалась сфера рекламного сопровождения предоставления гражданам товаров и услуг²¹, в области санитарно-эпидемиологического благополучия граждан — сфера информационного обеспечения защиты здоровья населения²², в области защиты прав детей — сфера защиты от вредной информации²³. Информационным дефектом в сфере рекламы товаров и услуг, не обеспечивающим или даже угрожающим интересам граждан, является недостоверная и недобросовестная реклама (ст. 5 Федерального закона «О рекламе»), за распространение которой предусмотрена соответствующая юридическая ответственность. Особое внимание необходимо уделять информации, адресатом которой являются дети. Детская психика более чувствительная, чем взрослая, и в большей степени подвержена внешнему влиянию. Требуется обезопасить самих детей, их жизнь и здоровье. Детская бравада и стремление скорее повзрослеть толкают их к употреблению наркотических и психотропных средств, занятию экстремальными (чаще всего противозаконными) видами деятельности, способствуют отчуждению от семейных традиций и ценностей, превалированию в отношении к окружающим их людям культа силы. Задачи информационной безопасности по отношению к этому контингенту граждан заключаются, наряду с законодательными запретами, и в проведении воспитательных мер, обеспечивающих позитивную социализацию детей, формиро-

вание у них механизмов критической оценки получаемых сведений²⁴.

Своевременное и оперативное предоставление достоверных информационных ресурсов для обеспечения санитарно-эпидемиологического благополучия населения — залог его безопасности и здоровья²⁵. Именно здесь высока ответственность государственных структур, от которых зависит жизнь и здоровье жителей целых населенных пунктов и регионов. Масовость и ценность объекта угроз определяют важность профилактической работы по мониторингу чрезвычайных ситуаций и своевременного доведения информации об угрозе жизни и здоровью людей для предотвращения негативных последствий. В свою очередь, граждане должны иметь возможность самостоятельно получить от компетентных органов и организаций всю информацию, которая может каким-то образом обеспечить сохранение принадлежащих им ценностей, включая прежде всего их здоровье и жизнь, тем более что в силу ч. 3 ст. 41 Конституции РФ сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.

Большой объем, важность и долгосрочность задач по обеспечению информационной безопасности граждан предполагают необходимость консолидации и активизации усилий государства в этом направлении. В связи с этим вполне уместны предложения А. А. Чеботаревой по созданию и закреплению «правового

судами Закона РФ «О средствах массовой информации» ; постановление Пленума Верховного Суда РФ от 13.12.2012 № 35 «Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

²¹ Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

²² Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

²³ Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

В последнее время стала актуальной проблема сексуального просвещения несовершеннолетних, в связи с чем 5 декабря 2022 г. была внесена новая редакция ст. 6.21 КоАП РФ о запрете пропаганды информации о смене пола, о нетрадиционных сексуальных отношениях и (или) предпочтениях.

²⁴ См.: Концепция информационной безопасности детей, утв. распоряжением Правительства РФ от 02.12.2015 № 2471-р // URL: pravo.gov.ru (дата обращения: 01.10.2023).

²⁵ Среди такого рода информационных ресурсов статья 8 Федерального закона «О санитарно-эпидемиологическом благополучии населения» выделяет информацию о состоянии среды обитания, качестве и безопасности продукции производственно-технического назначения, пищевых продуктов, товаров для личных и бытовых нужд, о потенциальной опасности для здоровья человека выполняемых работ и оказываемых услуг.

механизма мониторинга состояния защищенности личности от внутренних и внешних угроз в информационной сфере, а также учреждения института Уполномоченного по защите прав личности в информационной сфере при Президенте РФ»²⁶. Это позволит систематизировать разнообразную государственную и общественную деятельность по выявлению и оценке информационных ресурсов, угрожающих безопасности граждан, институализировать ее организационную основу, придать ей более предметный, целенаправленный характер, консолидировать с другими важными направлениями государственной деятельности.

Как в любом ином государстве, режим информационной гарантированности и безопасности граждан в России непосредственно связан с режимом чрезвычайных ситуаций, которые могут быть вызваны военными действиями, природными катаклизмами, техногенными авариями, эпидемиями, массовыми беспорядками и иными чрезвычайными событиями, повлекшими массовое ухудшение состояния благополучия граждан на определенной территории государства, угрожающими их жизни и здоровью. На этот счет существует целый ряд федеральных актов, предписывающих алгоритм действий каждого уровня представителей публичной власти. Не последнее место среди этих мер отведено вопросам информационного обеспечения, предназначенного для урегулирования этих ситуаций в режиме, который будет максимально способствовать прежде всего интересам самих граждан.

Так, в условиях режима военного положения вводится военная цензура за почтовыми отправлениями и сообщениями, передаваемыми с помощью телекоммуникационных систем. В режиме контртеррористической операции вводится контроль телефонных переговоров и иной информации, передаваемой по каналам телекоммуникационных систем. При введении чрезвычайного положения, вызванного событиями социального характера, мерами ограничения информационных свобод граждан могут быть ограничение свободы печати и других средств массовой информации путем введения предварительной цензуры с указанием условий и порядка ее осуществления, а также

временное изъятие или арест печатной продукции, радиопередающих, звукоусиливающих технических средств, множительной техники, установление особого порядка аккредитации журналистов.

Последние события, связанные с военной операцией России на Украине, актуализировали проблемы информационного противодействия воюющих сторон. Провокационная и сфальсифицированная информация противника, особенно в Интернете, наносит порой не менее тяжелый урон нашим интересам, чем его военные и террористические операции. Неслучайно эту войну называют гибридной, понятие которой связано с тем, что нападающая сторона, не прибегая к прямому вторжению, подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойн. Принятый еще до начала военной операции на Украине федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации впервые собрал и ранжировал субъекты и объекты информационной инфраструктуры в зависимости от областей их использования (социальной, политической, экономической, экологической, а также с точки зрения оборонной, государственной и общественной безопасности)²⁷.

Само понятие объекта критической информационной инфраструктуры связано с информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления субъектов критической информационной инфраструктуры, а также с управленческими, технологическими, производственными, финансово-экономическими и (или) иными процессами в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в вышеуказанных областях их использования. Перечень сфер критической информационной инфраструктуры включает в себя: здравоохранение, науку, транспорт, связь, энергетику, банковскую сферу и иные сферы финансового рынка, топливно-энергетический комплекс, области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышлен-

²⁶ Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : автореф. дис. ... д-ра юрид. наук. М., 2017. С. 17.

²⁷ Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

ности (п. 8 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»)²⁸.

Детализация положений данного закона осуществляется в постановлении Правительства РФ²⁹, где представлены три категории значимости объектов критической информационной инфраструктуры. При этом категория (первая — самая высокая, вторая и третья) устанавливается правительственной комиссией по категорированию с учетом показателей значимости объектов критической информационной инфраструктуры, установленных в каждой отраслевой сфере объектов информационной инфраструктуры.

Характерно, что ранжирование этих категорий в каждой области использования (социальной, политической, экономической и т.д.) зависит как от характера причиненного ущерба (угрозы его причинения), так и от степени его распространенности (чем большему количеству людей этот ущерб причинен, тем выше категория). Следует иметь в виду, что владельцами (субъектами) этих информационных ресурсов являются не только государственные органы и учреждения, но и юридические лица, инди-

видуальные предприниматели, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы и сети.

Все эти собственники и владельцы должны сознавать, что в условиях сбоя или повреждения их информационных систем происходит массовое, порой необратимое нарушение прав и свобод граждан, причем в наиболее важных и существенных для жизнеобеспечения сферах. Острая потребность в высоких компьютерных технологиях и программах, которые используются в современных информационных системах, отсутствие или дефицит соответствующих специалистов в IT-индустрии, массовый отток с отечественного рынка иностранных промышленных продуктов в области создания компьютерных программ, производства интеллектуальных продуктов, изделий и комплектующих, несомненно, негативным образом влияет на уровень информационной безопасности российского государства и наших граждан.

Эта задача требует комплексного решения, но консолидировать весь этот процесс можно только при помощи своевременно принятых и эффективных законодательных актов.

СПИСОК ЛИТЕРАТУРЫ

Афанасьева В. Р. Проблемы и пути решения информационной безопасности в банковской сфере // Эволюция российского права : материалы XVII Международной научной конференции, Уральский государственный университет. Екатеринбург, 2019. С. 395–397.

Ганеев А. А. Кибербезопасность в условиях агрессивной внешней информационной среды // Сборник материалов международного форума / под общ. ред. Р. Н. Минниханова. Казань, 2022. С. 286–290.

Герашенко А. Диалектика приватности в условиях развития информационной безопасности // Международное правосудие. 2022. № 4. С. 51–72.

Колосова Т. Е. Проблемы реализации охранительной функции государства в сфере защиты прав человека в цифровом пространстве // Актуальные проблемы государства и права. 2022. Т. 6. № 2. С. 151–157.

Корнев Г. П. Дезинформация и заблуждение в информационном пространстве // Труды III Всероссийской научной конференции. М., 2021. С. 210–214.

Кривоухов А. А. К оценке уровня безопасности личности в информационно-коммуникационной среде со стороны криминала // Мир науки. Социология, филология, культурология. 2020. Т. 11. № 1. С. 3–10.

Подупейко А. А. Некоторые вопросы обеспечения конституционных прав и свобод личности в условиях цифровой трансформации // Актуальные проблемы достижения целей устойчивого развития в условиях цифровой трансформации государства и права в Республике Беларусь : материалы республиканской научно-практической конференции. Минск, 2022. С. 316–317.

²⁸ Данный перечень был дополнен 10 июля 2023 г. сферой регистрации прав на недвижимое имущество и сделок с ним.

²⁹ Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // URL: pravo.gov.ru (дата обращения: 01.10.2023).

Пономарев М. В. Цифровая компетенция граждан как фактор информационной безопасности современного мегаполиса // Правовые аспекты безопасности города Москвы: исторический опыт, актуальные тенденции и перспективы : материалы круглого стола, проведенного в рамках XVI Фестиваля науки города Москвы. М., 2022. С. 113–119.

Хабриева Т. Я. Доклад на Петербургском международном юридическом форуме «Конституционный контроль: развиваем доктрину и совершенствуем практику» // Российская юстиция. 2023. № 6. С. 3–8.

Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : автореф. дис. ... д-ра юрид. наук. М., 2017. 55 с.

REFERENCES

Afanasieva VR. Problems and solutions of information security in the banking sector. In: The Evolution of Russian Law. Proceedings of the 27th International Scientific Conference, Ural State University. Ekaterinburg; 2019. Pp. 395–397. (In Russ.).

Chebotareva AA. Legal provision of information security of the individual in the global information society. The author's abstract of Dr. Diss. (Law). Moscow; 2017. (In Russ.).

Ganeev AA. Cybersecurity in an aggressive external information environment. In: Minnikhanov RN, editor. Collection of papers of the International forum. Kazan; 2022. Pp. 286–290. (In Russ.).

Gerashchenko A. The dialectic of privacy in the context of information security development. *International justice*. 2022;4:51-72. (In Russ.).

Khabrieva TYa. Report at the St. Petersburg International Legal Forum «Constitutional Control: developing doctrine and improving practice». *The Russian justice system*. 2023;6:3-8. (In Russ.).

Kolosova TE. Problems of realization of the protective function of the state in the field of human rights protection in the digital space. *Aktualnye problemy gosudarstva i prava [Current Issues of the State and Law]*. 2022;6(2):151-157. (In Russ.).

Kornev GP. Misinformation and misconception in the information space. Papers of the 3d All-Russian Scientific Conference. Moscow; 2021. Pp. 210–214. (In Russ.).

Krivoukhov AA. To the level of personal security assessment in the information and communication environment from the criminal side. *The world of science. Sociology, philology, cultural studies*. 2020;11(1):3-10. (In Russ.).

Podupeyko AA. Some issues of ensuring the constitutional rights and freedoms of the individual in the context of digital transformation. Current problems of achieving sustainable development goals in the context of digital transformation of the state and law in the Republic of Belarus. Proceedings of the Republican scientific and practical conference. Minsk; 2022. Pp. 316–317. (In Russ.).

Ponomarev MV. Digital competence of citizens as a factor of information security in a modern megalopolis. Legal aspects of the security of the city of Moscow: historical experience, current trends and prospects. Proceedings of the round table held as part of the 16th Moscow Science Festival. Moscow; 2022. Pp. 113–119. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Уваров Александр Александрович, доктор юридических наук, профессор, профессор кафедры государственно-правовых дисциплин Всероссийского государственного университета юстиции д. 2, корп. 1, Азовская ул., г. Москва 117638, Российская Федерация
uvarov.al@mail.ru

INFORMATION ABOUT THE AUTHOR

Alexander A. Uvarov, Dr. Sci. (Law), Professor, Professor, Department of State and Legal Disciplines,
the All-Russian State University of Justice
2, building 1, Azovskaya St., Moscow 117638, Russian Federation
uvarov.al@mail.ru

*Материал поступил в редакцию 4 октября 2023 г.
Статья получена после рецензирования 4 ноября 2023 г.
Принята к печати 18 декабря 2023 г.*

*Received 04.10.2023.
Revised 04.11.2023.
Accepted 18.12.2023.*