УДК 34:004.056.5(045)

А.К. Дубень

АСПЕКТЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭПОХУ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ВОЙН

Статья посвящена актуальным вопросам обеспечения информационной безопасности на современном этапе в условиях новых вызовов, угроз и рисков. В условиях развития информационного общества важную значимость приобретает исследование направлений усиления информационной безопасности в различных сферах жизнедеятельности личности, общества и государства. Сформировано значение информации, выявлены основные направления обеспечения информационной безопасности в цифровой сфере. В работе установлено, что на сегодняшний день информационная безопасность выступает в качестве приоритетов планирования в области национальной безопасности, тем самым внутренняя и внешняя политика государства осуществляет защиту информации и информационной инфраструктуры. Выявлен рост информационных угроз в глобальных изменениях интеграционных процессов в сфере обеспечения информационной безопасности, который поспособствовал отечественного законодателя к принятию ряда нормативных актов, направленных на формирование и развитие системы национальной информационной безопасности. В статье рассматриваются современные виды информационных угроз, при этом рассмотренные угрозы на сегодняшний день приобретают актуальность, поскольку нынешняя повестка дня международного права позволяет сделать вывод о том, что в отношении Российской Федерации ведется информационное противоборство. В процессе исследования автор сделал вывод, что рассмотренные проблемы в области обеспечения информационной безопасности и новые типы угроз на современном этапе требуют дальнейшего научного осмысления, в свою очередь, система информационного права в настоящее время находится в процессе активной трансформации, с увеличением количества кибератак государство предпринимает все необходимые меры по защите отечественных информационных ресурсов и критически важных информационных объектов.

Ключевые слова: информационное право, трансформация права, цифровизация, информационная безопасность, вызовы и угрозы, кибератаки, кибервойны, система публичной власти, цифровые технологии, информатизация.

DOI: 10.35634/2412-9593-2022-32-6-1064-1068

Развитие процессов цифровой трансформации, формирование информационного пространства и информатизация общественно-политической жизни значительно повысили роль и значимость информационного права[1]. Вместе с тем информация как источник сведений порождает негативные факторы в виде новых вызов, угроз и рисков для национальной и международной информационной безопасности, требующие активного реагирования. Современные угрозы информационной безопасности обуславливают потребность в системной модернизации правового регулирования информационной безопасности[2].

Согласно Стратегии национальной безопасности Российской Федерации информационная безопасность является одним из элементов национальной безопасности. Таким образом, информационная безопасность является одним из девяти ключевых приоритетов, поскольку внедрение в жизнь динамичного характера развития информационных технологий, внедрение прорывных информационных процессов влияют на благосостояние граждан и отражаются на правовой системе. Согласно п. 25 вышеуказанного документа одним из ключевых национальных интересов является развитие безопасного информационного пространства, тем самым не допуская в будущем информационные риски и угрозы[3]. Таким образом, Российская Федерация определяет информационную безопасность в качестве приоритетов планирования в области национальной безопасности.

На сегодняшний день обеспечение информационной безопасности, включая сетевую и цифровую безопасность, является приоритетной и одной из ключевых задач как на национальном, так

[1] Камалова Г.Г. Информация как правовая категория: развитие концептуальных подходов // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2017. Т. 3 (69), № 3. С. 185.
[2] Полякова Т.А., Минбалеев А.В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С. 108.
[3] Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. 2). Ст. 5351.

и на международном уровне. Как уже было ранее отмечено, экспоненциальное развитие цифровых, прорывных и конвергентных технологий несет за собой колоссальные риски и угрозы. На наш взгляд, данную проблему можно устранить путем организационно-технической и правовой защиты в информационном пространстве.

В этой связи в условиях геополитических изменений, трансформации права и цифровизации всех сфер жизнедеятельности, включая правовые процессы конституционализации и институционализации, в праве необходимы научные исследования и проработки новых подходов к систематизации информационного права. Важно отметить, что обеспечение информационной безопасности в современных условиях связаны с проблемами действия норм международного права и нерешенности на законодательном уровне информационно-правовых вопросов в национальной системе права. В связи с этим стоит согласиться с позицией профессора П.У. Кузнецова: «Перед правовой системой стоит непростая программная задача осмыслить цифровые реалии и на основе существующих традиций создать новые правовые средства регулирования общественных отношений и обеспечения развития страны»[4].

В информационном законодательстве существует ряд проблем при обеспечении безопасности: кибератаки, общественно-опасные деяния с использованием информационных средств, применение искусственного интеллекта и робототехники в преступных целях. Следует признать, что система правового регулирования в области обеспечения информационной безопасности в полной мере не соответствует требованиям времени и на сегодняшний день развивается несистематично, что особенно нехарактерно для исполнения стратегических актах, национальных проектов и концептуальных документов, связанных с информационной сферой. К примеру, в связи с принятием ряда нормативных актов понятие «информационная безопасность», потеряло свое значение в современных условиях развития информационных технологий, повышения требований по защите безопасности и основных направлений развития государственной политики в данной сфере. В связи с этим, рассмотрев правовые аспекты правового обеспечения информационной безопасности, следует в качестве рекомендаций сформулировать определение информационной безопасности. Информационная безопасность – состояние защищенности субъектов от внутренних и внешних угроз, связанных с применением информационных технологий в различных целях, при котором обеспечивается защита конституционно значимых ценностей в целях укрепления суверенитета Российской Федерации в информационном пространстве.

На современном этапе научная доктрина рассматривает информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних угроз, обеспечивая при этом конституционные права человека и гражданина, включая достойное качество жизни, суверенитет, устойчивое социально-экономическое развитие и иные конституционные гарантии[5].

Вместе с тем кибератаки и угрозы осуществляются общественно-опасными и противоправными действиями, которые в последствии наносят вред правам, свободам и интересам граждан, возникающими в результате несовершенства правового регулирования информационной безопасности, включая коллизии и пробелы в законодательстве, а также злоупотребления правами и свободами, которые в последствии нарушают общественный правопорядок.

Рассмотренные информационные угрозы на сегодняшний день приобретают актуальность, поскольку нынешняя повестка дня международного права позволяет сделать вывод о том, что в отношении Российской Федерации ведется информационная война. Стоит обратить внимание, что в 2022 году Российская Федерация в условиях геополитических изменений и ведения информационных войн осуществляет на постоянной основе работу центров интернет-технологий по приведе-

[4] Кузнецов П.У. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 6. С. 156.

[5] См., например: Бачило И.Л. Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 5-16; Полякова Т.А., Камалова Г.Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2 (68). С. 112-121; Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. … докт. юрид. наук. 2020. 472 с.; Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … докт. юрид. наук. 2008. 438 с.; Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. М., 2002. 289 с.

нию международных норм в национальные стандарты обеспечения нейтралитета в информационной сфере[6]. Большинство ученых считают, что данные меры позволят в дальнейшем эффективно обеспечить международное и межгосударственное сотрудничество в сфере обеспечения информационной безопасности[7].

Можем констатировать, что рост информационных угроз в глобальных изменениях интеграционных процессов в сфере обеспечения информационной безопасности поспособствовал отечественного законодателя к принятию ряда нормативных актов, направленных на формирование и развитие системы национальной информационной безопасности.

Среди рисков, угроз и вызовов, препятствующих реализации прав и свобод человека и гражданина в цифровом пространстве, полагаем, можно выделить кибератаки на различные информационные ресурсы в эпоху современных информационных войн. Из-за прогрессивного характера развития технологий и расширения информационных ресурсов общество сталкивается с большим количеством угроз, которых ранее не было. Как отмечают О. И. Филонова, А. Я. Неверов, в современном мире все чаще наблюдаются тенденции к увеличению роста компьютерных атак и распространение их по всему миру, при этом прослеживается рост кибератак, направленных на отдельные органы государственной власти и их информационные ресурсы[8]. К примеру, в 2021 году установлено беспрецедентное количество атак на справочно-информационный интернет-портал «Госуслуги»[9]. Преступники в информационной сфере используют ряд направлений для осуществления киберратак с помощью новых методов и приемов для достижения преступных целей. При этом распределенные кибератаки (DoS-атаки) в большинстве случаев применяются с целью отключения систем и сетей. Так, представители кредитной организации «Сбербанк» отмечают, что в первом полугодии 2022 года информационные ресурсы банка выдержали более 800 DDOS-атак, данное количество равно всем DDOS-атакам, которые имелись в компании за последние 5 лет[10]. Как отмечают специалисты «Лаборатории Касперского», в 2022 году кибератаки на российские организации выросли в восемь раз по сравнению с аналогичным периодом в прошлом году, причем больше всего атак совершалось на банки – 35 % от общего числа кибератак[11].

Президентом России В.В. Путиным не раз отмечалось, что: «новые технологические решения порождают новые риски. Мы видим, что глобальное цифровое пространство нередко становится площадкой для жесткого информационного противоборства, для нечестной конкуренции и кибератак»[12]. В этой связи нельзя не отметить, что Стратегия национальной безопасности Российской Федерации отличается некоторыми политическими аспектами, соответствующими сложившейся политической конъюнктуре взаимоотношений между Россией и иными странами. Таким образом, указанное обстоятельство свидетельствует о мотивах принятия ряда нормативно-правовых актов с целью обеспечения информационной безопасности.

В соответствии с Указом Президента Российской Федерации «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» основными задачами государственной системы по недопущению компьютерных атак на информационные ресурсы государства являются: постоянный прогноз ситуации в области обеспечения информационной безопасности; взаимодействие всех

---

[6] См.: ООН просят устанавливать цифровой нейтралитет в период вооруженных конфликтов // Интернет-издание «Ведомости». 2022. 8 марта. URL: https://www.vedomosti.ru/society/articles/2022/03/08/912604-oon-tsifrovoi-neitralitet?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews%2Fsearch%3Ftext%3D (дата обращения: 06.04.2022).

[7] См.: ООН просят устанавливать цифровой нейтралитет в период вооруженных конфликтов.

[8] Филонова О.И., Неверов А.Я. Проблемы развития публичного права в условиях формирования информационного общества // Сборники Президентской библиотеки. Вып. 11: Право и информация: вопросы теории и практики : сб. матер. междунар. науч.-практ. конф. / науч. ред. Н.А. Шевелева, д-р юрид. наук, проф. 2022. С. 165.

[9] Минцифры рассказало о мощной кибератаке на «Госуслуги» // РИА Новости. URL: https://ria.ru/20211111/kiberataka-1758635270.html (дата обращения: 30.09.2022).

[10] «Сбер» и его «дочки» за последний квартал испытали 800 кибератак // РИА Новости. URL: https://ria.ru/20220906/kiberataki-1814707291.html (дата обращения: 05.10.2022).

[11] «Сбер» оценил число участвующих в кибервойне с Россией хакеров в 100 тыс. // Официальный сайт РБК. URL: https://www.rbc.ru/business/12/05/2022/627d5b339a79473cb7c54d9b(дата обращения: 05.10.2022).

[12] Заседание Совета Безопасности // Сайт Президента РФ. Новости, выступления и стенограммы. 26 марта 2021 г. URL.: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 28.09.2022).

информационных ресурсов по защите информации; общее решение задач по выявлению, предупреждению и устранению последствий компьютерных атак; своевременный контроль по степени защищенности информационных ресурсов государства[13]. В рамках указанных задач следует отметить, что с увеличением количества кибератак государство предпринимает все необходимые меры по защите отечественных информационных ресурсов и критически важных информационных объектов, в этой связи полностью поддерживаем позицию Т.А. Поляковой, Г.Г. Камаловой об усилении законодательных требований к защите конфиденциальности цифровых данных[14].

Рассмотренные проблемы в области обеспечения информационной безопасности ставят вопрос о внедрении технических и организационно-технических систем мониторинга безопасности в информационной сфере, которые выступили бы вспомогательной системой защиты в условиях новых вызовов, угроз и рисков[15]. Данные меры, на наш взгляд, позволят осуществлять более своевременный и эффективный способ контроля защищенности информационной системы и инфраструктуры Российской Федерации, тем самым позволят нейтрализовать информационные риски и угрозы путем оперативного их устранения. Следовательно, основной задачей является необходимость внедрения самостоятельных и независимых средств мониторинга обеспечения информационной безопасности Российской Федерации.

Подведем итог. Рассмотренные проблемы в области обеспечения информационной безопасности и новые типы угроз на современном этапе требуют дальнейшего научного осмысления с позиции информационного права, поскольку в условиях новых вызовов и рисков, цифровой трансформации и цифровизации права данные меры влияют на систему права. Выявлено, что развитие безопасного информационного пространства, защита населения от деструктивного информационного воздействия, охрана информационных ресурсов и недопущение информационных угроз являются одной из основных задач государства в условиях ведения информационных войн. Считаем, что предложенные меры позволят в дальнейшем определить векторы развития государственной политики Российской Федерации и развитие всей правовой системы в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И.Л. Понятийный аппарат информационного права и система обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 5-16.
2. Кузнецов П.У. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 6. С. 154-161.
3. Камалова Г.Г. Информация как правовая категория: развитие концептуальных подходов // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2017. Т. 3 (69). № 3. С. 185-192.
4. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: Дисс. ... д-ра юрид. наук. 2020. 472 с.
5. Мошак Н.Н., Евсейко К.В., Логинцев А.В. Проблемы защиты информационно-телекоммуникационной инфраструктуры РФ от кибератак // В сб.: Региональная информатика и информационная безопасность: сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2017. С. 31-36.
6. Полякова Т.А., Камалова Г.Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2 (68). С. 112-121.
7. Полякова Т.А., Минбалеев А.В. Понятие и правовая природа «цифровой зрелости» // Государство и право. 2021. № 9. С. 107-116

[13] Указ Президента РФ от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СЗ РФ. 2017. № 52 (Часть I). Ст. 8112.

[14] Полякова Т.А., Камалова Г.Г. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») // Правовое государство: теория и практика. 2022. № 2 (68). С. 117.

[15] Мошак Н.Н., Евсейко К.В., Логинцев А.В. Проблемы защиты информационно-телекоммуникационной инфраструктуры РФ от кибератак // В сб.: Региональная информатика и информационная безопасность: сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2017. С. 33.

8. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: Дисс. ... д-ра юрид. наук. 2008. 438 с.
9. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. М., 2002. 289 с.
10. Филонова О.И., Неверов А.Я. Проблемы развития публичного права в условиях формирования информационного общества // Сборники Президентской библиотеки. Вып. 11: Право и информация: вопросы теории и практики : сб. матер. междунар. науч.-практ. конф. / науч. ред. Н. А. Шевелёва, д-р юрид. наук, проф. 2022. С. 164-168.

Поступила в редакцию 12.09.2022

Дубень Андрей Кириллович, научный сотрудник
ФГБУН Институт государства и права Российской академии наук
119019, Россия, г. Москва, ул. Знаменка, 10
E-mail: k.duben@mail.ru

A.K. Duben

ASPECTS AND THREATS OF INFORMATION SECURITY IN THE ERA OF MODERN INFORMATION WARS

DOI: 10.35634/2412-9593-2022-32-6-1064-1068

The article is devoted to topical issues of ensuring information security at the present stage in the context of new challenges, threats and risks. In the context of the development of the information society, the study of the directions of strengthening information security in various spheres of life of the individual, society and the state is of great importance. The value of information is formed, the main directions of ensuring information security in the digital sphere are identified. It is established in the work that today, information security acts as a priority of planning in the field of national security, thereby the internal and foreign policy of the state protects information and information infrastructure. The growth of information threats in global changes in integration processes in the field of information security has been revealed, which has contributed to the adoption of a number of regulations by the domestic legislator aimed at the formation and development of the national information security system. The article deals with modern types of information threats, while the threats considered today are becoming relevant, since the current agenda of international law allows us to conclude that an information confrontation is being conducted against the Russian Federation. In the course of the research, the author concluded that the considered problems in the field of information security and new types of threats at the present stage require further scientific understanding, in turn, the information law system is currently in the process of active transformation; with an increase in the number of cyber attacks, the state is taking all necessary measures to protect domestic information resources and critical information objects.

Keywords: information law, transformation of law, digitalization, information security, challenges and threats, cyberattacks, cyber wars, public power system, digital technologies, informatization.

Received 12.09.2022

Duben A.K., researcher
Institute of State and Law of the Russian Academy of Sciences
Znamenka st., 10, Moscow, Russia, 119019
E-mail: k.duben@mail.ru