Г. З. Мансуров

ПРАВО ЦИФРОВОЙ БЕЗОПАСНОСТИ

Учебник

DirectMEDIA

Г. З. Мансуров

Право цифровой безопасности

Учебник

DirectMEDIA
Москва
2022

УДК 004.056(075)
ББК 16.8я73
М23

Рекомендован УМК Института государственного, муниципального управления и права Уральского государственного экономического университета (протокол № 9 от 28.02.2022 г.)

Мансуров, Г. З.

М23 Право цифровой безопасности : учебник / Г. З. Мансуров. — Москва : Директ-Медиа, 2022. — 148 с.

ISBN 978-5-4499-3061-3

Одним из важнейших направлений развития современных общественных отношений является цифровизация. Кроме очевидных достоинств, процесс цифровизации имеет также и определенные недостатки. Одним из самых серьезных негативных последствий цифровой трансформации является многократно возросшая опасность угрозы цифровой безопасности России и ее граждан. Целью данного учебного издания является анализ наиболее серьезных цифровых угроз и, соответственно, правовых способов их минимизации или ликвидации.

Учебник адресован студентам, обучающимся по направлению подготовки «юриспруденция» и направлению подготовки «экономика» (профили «экономическая безопасность» и «бизнес-безопасность и управление рисками»). Он также будет полезен специалистам в сфере информационно-коммуникационных технологий.

УДК 004.056(075)
ББК 16.8я73

ISBN 978-5-4499-3061-3

Оглавление

Введение

Данный учебник является первым учебным изданием по праву цифровой безопасности. Объективная необходимость введения одноименной учебной дисциплины и, соответственно, подготовки данного учебного издания обусловлена процессом цифровой трансформации и, соответственно, возникающими специфическими угрозами.

Учебник адресован студентам, обучающимся по направлению подготовки «Юриспруденция» и направлению подготовки «Экономика» (профили «Экономическая безопасность» и «Бизнес-безопасность и управление рисками») для более углубленного изучения правовых аспектов обеспечения цифровой безопасности. Также будет полезен специалистам в сфере информационно-коммуникационных технологий.

Содержание учебника соответствует требованиям рабочей программы дисциплины «Право цифровой безопасности».

Право цифровой безопасности является новым, только складывающимся *комплексным институтом права экономической безопасности* и включает в себя нормы разных отраслей права, самыми важными из которых являются нормы конституционного, гражданского, административного, уголовного и международного права.

Учебник подготовлен на основе концепции права экономической безопасности, разработанной автором в 2011–2021 годах[1].

Следует учитывать, что право цифровой безопасности является дальнейшим развитием права информационной безопасности. Как отмечается в литературе, «Сам термин “цифровая

[1] См. напр.: Мансуров Г. З. Международные договоры в системе регуляторов обеспечения экономической безопасности / Экономико-правовые проблемы обеспечения экономической безопасности. Материалы III Международной научно-практической конференции; отв. ред. Е. Б. Дворядкина, Г. З. Мансуров. — 2020. — С.185–187; он же. Правовые проблемы обеспечения экономической безопасности в условиях цифровизации / Экономико-правовые проблемы обеспечения экономической безопасности. Материалы II Всероссийской научно-практической конференции. — 2019. — С. 208–212; он же. Новый закон о безопасности и старые проблемы законодательства о безопасности // Управленец. — 2011. — № 1–2 (17–18). — С. 48–52; он же. Законодательство о безопасности: некоторые проблемы дальнейшего совершенствования // Безопасность бизнеса. — 2011. — № 3. — С. 10–14 и др.

безопасность" (*или же информационная безопасность* — курсив мой — *Г. М.*) означает такое регулированное правом состояние защищенности электронной информации, при котором отсутствуют угрозы ее безопасности»[2]. Данное обстоятельство обусловлено трендом на использование термина «цифровизация» для обозначения понятий информатизация, софтверизация и компьютеризация.

Задачей учебной дисциплины право цифровой безопасности является сжатое изложение основных доктринальных положений, содержания действующего законодательства и судебно-арбитражной практики в сфере обеспечения безопасности цифровых отношений.

Учебное издание состоит из двух частей. *Общая часть* состоит из трех глав и включает в себя общие положения права цифровой безопасности. В *первой главе* рассматриваются признаки цифровизации и безопасности как экономико-правовых явлений. Дается характеристика права цифровой безопасности, источников правового регулирования. Как известно, цифровые отношения могут возникать только в Интернете. Поэтому *вторая глава* полностью посвящена правовым проблемам, возникающим в сфере интернет-отношений: информация как объект правового регулирования, понятие и признаки информационно-коммуникационных сетей. Особое внимание, в силу большого количества судебных споров, уделено сведениям конфиденциального характера и их разновидности — персональным данным.

Третья глава учебника является центральной. В ней изложена основная информация о мерах правового воздействия на риски и угрозы в цифровой сфере. Отдельно, в силу их чрезвычайной актуальности, выделены угрозы в социальных сетях (параграф 2). В *третьем параграфе* содержится общая характеристика правового воздействия на цифровые угрозы.

Вся *особенная часть* учебника представляет собой детализацию положений, содержащихся в третьем параграфе третьей главы, по отраслям российского права: уголовно-правовая ответственность в сфере цифровых отношений (глава 4), ад-

[2] Елизарова Е. О., Настич В. М., Чекулаев С. С. Правовое регулирование цифровой безопасности в России и странах АТР и ее соотношение с кибербезопасностью // Юридическая наука. — 2020. — № 6. — С. 42.

министративно-правовая ответственность (глава 5), гражданско-правовая ответственность (глава 6) и международно-правовые механизмы обеспечения цифровой безопасности (глава 7).

Литература

1. Мансуров Г. З. Цифровое право. — Екатеринбург: Изд-во УрГЭУ, 2020.

2. Пучков В. О. Цивилистическая доктрина цифровой эпохи: методологические, теоретические и прикладные проблемы. Монография / под ред. В. С. Белых. — М.: Изд-во «Проспект», 2020.

3. Санникова Л. В., Харитонова Ю. С. Цифровые активы: правовой анализ. Монография. — М.: Изд-во «4 Принт», 2020.

4. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — М.: Изд-во «Проспект», 2020.

5. Цифровое право в банковской деятельности: сравнительно-правовой аспект. Монография / отв. ред. Л. Г. Ефимова. — М.: Изд-во «Проспект», 2021.

Общая часть

Глава 1. Понятие и общая характеристика права цифровой безопасности как института законодательства, раздела юриспруденции и учебной дисциплины

1.1. Понятие и общая характеристика цифровизации

В настоящее время, несмотря на широкое применение термина «цифровизация» («цифровая трансформация»), отсутствует его общепринятое определение. Наиболее часто под *цифровизацией* понимается преобразование информации в цифровую форму. Так, например, согласно постановлению Правительства РФ от 3 декабря 2009 г. № 985 «О федеральной целевой программе "Развитие телерадиовещания в Российской Федерации на 2009–2018 годы"», предусматривается обеспечение условий для перехода на цифровой формат распространения телевизионных программ. То есть, в данном документе под цифровизацией понимается переход с аналоговой формы передачи информации на цифровую. И, соответственно, термином «цифровизация» обозначается *способ передачи информации в эфире*. Поэтому термин «цифра» используется не как знак, указывающий на количество или порядок, а как обозначение результата особой технологии записи и чтения информации[3]. Как отмечается в литературе, исторически так сложилось, что *малознакомый математический термин* «*дискретный*», *заменили на более привычный термин* «*цифровой*», игнорируя при этом то, что в дискретном понимании цифр всего две — 0 и 1.

Во втором же случае термин «цифровизация» понимается совершенно иначе. Так, например, согласно пункту 6.3 Основных направлений деятельности Правительства Российской Федерации на период до 2024 года (утв. Правительством РФ 29 сентяб-

[3] Такое же понимание данного термина содержится в ряде международных актов. См. напр.: Решение Совета глав правительств СНГ «О деятельности Регионального содружества в области связи» от 31 мая 2013 г.; Решение Совета глав правительств СНГ «О Стратегии сотрудничества государств-участников СНГ в построении и развитии информационного общества на период до 2025 года и Плане действий по ее реализации» от 28 октября 2016 г. и др.

ря 2018 г.), будут осуществляться *меры по внедрению цифровых технологий и платформенных решений* («*цифровизации*») в практическую деятельность органов государственного управления федерального, отраслевого и регионального уровней[4].

В ряде случаев для обозначения преобразования информации в цифровую форму вместо термина «цифровизация» используются и другие:

1) *информатизация* — согласно отмененному в настоящее время федеральному закону об информации, информатизации и защите информации, под информатизацией понимается организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

В литературе отмечается, что этот термин в свое время нашел широкое распространение лишь в России и Китае. Это было связано, во-первых, с недостаточной разработанностью в 1980–1990-х годах глоссария по тематике «информационные технологии» и «информационное общество», во-вторых, с некоторыми специфическими особенностями развития информационно-коммуникационных технологий в этих странах. Они характеризовались высоким уровнем развития прикладных и специализированных аппаратно-программных комплексов и крайне слабой телекоммуникационной инфраструктурой, которая становилась тормозом гармоничного развития информационного общества[5];

2) *софтверизация* (от *англ*. software — программное обеспечение) — термин, означающий превращение в программу всего, что может быть лишено физической оболочки или физического воплощения;

---

[4] Сходные международно-правовые акты: Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года»; Решение Евразийского межправительственного совета от 9 августа 2019 г. № 8 «О паспорте проекта “Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий”» и др.

[5] https://luna.ovh/planeta/tab/ru/информатизация/92855ad420d0cda45018e94bf8be64df6201fd89

3) *компьютеризация* — внедрение электронно-вычислительной техники во все сферы общественных отношений.

В силу вышеизложенного очевидно, что выработать единое понимание содержания термина «цифровизация» уже не представляется возможным. Поэтому, с учетом содержания принятых нормативных актов, необходимо *различать цифровизацию в узком и широком смыслах*.

Под цифровизацией *в узком смысле* следует понимать меры по внедрению платформенных решений. В силу того, что важнейшей платформой является блокчейн, *термин* «*цифровизация*» *в данном случае будет обозначать блокчейнизацию*. Под блокчейном в самом общем виде понимается программный продукт, позволяющий хранить данные и проводить транзакции через Интернет без посредников.

Содержание понятия «цифровизация» *в широком смысле*, с учетом содержания нормативных актов, является практически необъятным[6]. Самым распространенным примером цифровизации в широком смысле является обозначение способа передачи информации в эфире (т. н. цифровизация телевидения).

1.2. Общая характеристика понятия «безопасность»

Переходя к анализу проблем толкования понятия «безопасность» следует предварительно отметить, что *в юриспруденции его содержание претерпело определенную эволюцию*. Долгое время безопасность воспринималась исключительно как международно-правовая категория. Важность данной категории для международного публичного права обусловило выделение в его составе новой отрасли — *право международной безопас-*

[6] Так, например, согласно одному из ведомственных документов, под цифровизацией понимаются: (1) обслуживание средств печати и копирования данных; (2) услуги по предоставлению доступа в интернет, местной и междугородней связи; (3) приобретение (продление) программных средств защиты и (4) выполнение мероприятий по переходу Министерства на отечественное программное обеспечение (приказ Минвостокразвития России от 1 февраля 2018 г. № 19 «Об утверждении Плана информатизации Министерства Российской Федерации по развитию Дальнего Востока на 2018 финансовый год и плановый период 2019 и 2020 годов»).

ности[7]. Согласно лапидарному высказыванию автора названия данной отрасли С. А. Малинина, укрепление безопасности преследует цель сохранить государство как суверенное образование среди других государств[8]. Следует отметить, что до сих пор преобладающим в доктрине является понимание норм права международной безопасности как регулятора военно-политических отношений государств[9].

Однако в России, в отличие от некоторых других стран, со временем возобладало понимание безопасности преимущественно как *государственной* безопасности в смысле обеспечение правопорядка внутри государства и, в первую очередь, от внутренних врагов. Так, по мнению американского историка Р. Пайпса, функцией корпус жандармов Третьего Отделения Собственной Его Величества Канцелярии была защита государственной безопасности[10].

После краткого периода революционной эйфории, советская власть также осознала важность обеспечения государственной безопасности. Так, в обращение Центрального Комитета коммунистической партии к избирателям сказано, если внутренние враги советского народа малочисленны и бесчисленны, то поддерживающие их внешние враги представляют серьезную опасность. Чтобы *обезопасить нашу Родину от этой опасности*, нужно иметь, во-первых, хорошо организованные карательные органы, способные обезвредить шпионов, вредителей, диверсантов и других врагов советского народа; нужно иметь, во-вторых, Красную Армию, способную охранять советские границы от нападения извне; нужно иметь, наконец, хорошо продуманную и последовательно проводимую политику

---

[7] Лазутин Л. А. Размышления о праве международной безопасности // Российский юридический журнал. — 2013. — № 3. — С. 46–51; Филиппов О. А., Харисова З. И. Право международной безопасности: современное состояние и тенденции развития // Вестник Института права Башкирского государственного университета. — 2020. — № 1 (5). — С. 46–50 и др.

[8] Черниченко С. В. Теория международного права. В 2-х т. — М.: Изд-во «НИМП», 1999. — Т. 2. — С. 487 и др.

[9] Международное право. Учебник / отв. ред. Г. В. Игнатенко и О. И. Тиунов. — М.: Изд-во Норма-Инфра, 1999. — С. 431. Автор главы — Л. А. Лазутин.

[10] Пайпс Р. Россия при старом режиме. — М.: Изд-во «Независимая газета», 1993. — С. 380.

мира, способную разоблачать захватническую политику воинствующих кругов капиталистических стран[11]. Как отмечается в литературе, термин «государственная безопасность» был введен в нашей стране в 1934 г. при образовании в составе НКВД Главного управления государственной безопасности, которому были переданы функции ОГПУ при его ликвидации.

Принятие закона о безопасности[12] в 1992 году явилось *новым этапом в развитии законодательства о безопасности*. Очевидным достоинством данного документа является обозначение основных функций системы безопасности: (1) выявление и прогнозирование внутренних и внешних угроз жизненно важным интересам объектов безопасности; осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации; (2) создание и поддержание в готовности сил и средств обеспечения безопасности; (3) управление силами и средствами обеспечения безопасности в повседневных условиях и при чрезвычайных ситуациях; (4) осуществление системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации и (5) участие в мероприятиях по обеспечению безопасности за пределами Российской Федерации в соответствии с международными договорами и соглашениями, заключенными или признанными Российской Федерацией (ст. 9 Закона «О безопасности»).

Однако следует учитывать, что меры защиты от угроз безопасности как физическим, так и юридическим лицам содержатся практически во всех отраслях законодательства, а не только законодательства о безопасности. *Предметом же законодательства о безопасности являются действия публично-правовых субъектов по устранению угроз только неопределенному кругу лиц международными или государственными органами*. В ином случае применяются *меры защиты*, закрепленные

---

[11] Юридический словарь / под ред. С. Н. Братуся и др. — М.: Гос. изд-во юрид. лит-ры, 1953. — С. 114.

[12] Закон РФ от 5 марта 1992 г. № 2446-I «О безопасности» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. — № 15. — Ст. 769.) Заменен впоследствии на ФЗ от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (Собрание законодательства РФ, 2011. — № 1. — Ст. 2.)

нормами иных отраслей законодательства (например, отказ от выполнения работы, которая непосредственно угрожает жизни и здоровью работника — ст. 379 Трудового кодекса РФ, самозащита права — ст. 12 Гражданского кодекса РФ, необходимая оборона — ст. 37 Уголовного кодекса РФ и т. д.).

По этой причине следует учитывать многозначность понятия «безопасность» и, в частности, ее разновидности — *экономической безопасности*. Так, например, один из юрисдикционных органов, рассматривая дело, пришел к следующему выводу: «с учетом того, что банк размещает привлеченные денежные средства на определенных условиях (возвратность, платность, срочность), действия всех ответственных подразделений банка и лиц, привлекаемых банком к обеспечению *экономической безопасности* (курсив мой — *Г. М.*), направлены на соблюдение указанных условий, а именно: обеспечение возвратов выданных кредитов, своевременную уплату процентов за пользование кредитами, определение способности заемщика в установленный срок возвратить кредит»[13]. Очевидно, что в данном случае речь идет о предмете гражданского законодательства, а не законодательства о безопасности.

Понятие «экономическая безопасность» появилось в лексиконе российских ученых и практиков на рубеже XIX и XX веков. Оно было заимствовано из иностранной литературы и представляет собой синтетическую категорию, образованную на стыке двух научных областей — экономики и политологии[14].

Под *экономической безопасностью* принято понимать, во-первых, состояние экономики, обеспечивающее достаточный уровень социального, политического и оборонного существования и прогрессивного развития РФ, неуязвимость и независимость ее экономических интересов по отношению к возможным внешним и внутренним угрозам и воздействиям и, во-вторых,

---

[13] Постановление Семнадцатого арбитражного апелляционного суда от 31 октября 2008 г. № 17АП-7050/2008-АК по делу № А71-4353/2008. Постановлением ФАС Уральского округа от 12 февраля 2009 г. № Ф09-408/09-С3 этот документ оставлен без изменений // ИПБ «Консультант-плюс».

[14] Шестаковских М. Н. Экономическая безопасность: истоки и элементы / Актуальные проблемы и перспективы развития государственного управления: сб. ст. / под ред. С. Е. Прокофьева, О. В. Паниной, С. Г. Еремина. — М.: Юстицинформ, 2015.

состояние юридических экономических отношений, организационных связей, материальных и интеллектуальных ресурсов предприятия, при котором гарантируется стабильность его функционирования, финансово-коммерческий успех, прогрессивное научно-техническое и социальное развитие[15].

Таким образом, *угроза безопасности является объектом законодательства о безопасности при наличии двух одновременно совпадающих условий*: (*1*) *для ее устранения требуется вмешательство государственных органов и* (*2*) *неопределенных круг субъектов воздействия угрозы*.

Вышеизложенное представляется возможным продемонстрировать на примере продовольственной безопасности следующим образом: *предметом законодательства о продовольственной безопасности* являются (1) разработка и осуществление мер, направленных на предупреждение продовольственных кризисов, удовлетворение потребностей населения в жизненно важных продуктах и (2) регулирование мер воздействия в ситуации, в которой обеспечение населения жизненно важными продуктами питания находится под угрозой и в которой данная угроза может быть устранена только мерами государственного регулирования. По этой причине отношения по обеспечению продовольственной безопасности отдельных субъектов не является объектом законодательства о продовольственной безопасности. Соответственно, не могут быть предметом регулирования законодательства о безопасности, например, обеспечение продовольствием малоимущих граждан (предмет социального законодательства), ликвидация последствий неурожая у отдельных сельскохозяйственных товаропроизводителей (предмет предпринимательского законодательства) и т. д.

1.3. Право цифровой безопасности в системе российского права

Право цифровой безопасности является *комплексной отраслью законодательства*, то есть системой нормативных правовых актов, принятых в целях регулирования определенного вида общественных отношений. Основные отрасли зако-

[15] Дворядкина Е. Б., Силин Я. П., Новикова Н. В. Экономическая безопасность. Учебное пособие. — Екатеринбург: Изд-во УрГЭУ, 2016. — С. 18–19.

нодательства содержатся в Указе Президента РФ от 15 марта 2000 г. № 511 «О классификаторе правовых актов»[16]. Отличие отрасли законодательства от отрасли права заключается в том, что отрасль права имеет свой предмет и метод регулирования, а отрасль законодательства, регулируя определенные сферы общественных отношений, разграничиваются по предмету регулирования.

Как указывает В. Ф. Яковлев, само появление и существование комплексных нормативных актов и комплексных отраслей законодательства есть результат взаимодействия различных отраслей права в регулировании отношений определенной сферы общественной жизни[17]. Право цифровой безопасности включает в себя нормы отраслей права, анализ содержания которых производится в особенной части учебного пособия.

Как известно, нормы права классифицируются на регулятивные и охранительные. Первые устанавливают позитивные правила нормальных для общества отношений, вторые же устанавливают санкции. Очевидно, что *для обеспечения* цифровой *безопасности важнейшее значение имеет вторая разновидность норм*.

1.4. Право цифровой безопасности как учебная дисциплина

Как известно задачей любой юридической учебной дисциплины является сжатое изложение основных доктринальных положений, содержания действующего законодательства и судебно-арбитражной практики. Соответственно, в *состав учебной дисциплины* включена информация об основных отраслях российского права, обеспечивающих цифровую безопасность — гражданское право, административное право, уголовное право, трудовое право и процессуальное право. В силу большого значения для обеспечения цифровой безопасности России ситуации на мировом рынке, в учебном пособии содержится информация о нормах международного публичного права и международного частного права, ориентированных

[16] Собрание законодательства РФ, 2000. — № 12. — Ст. 1260.

[17] Гражданское право в системе права // Яковлев В. Ф. Избранные труды. — М.: Статут, 2012. — Т. 2: Гражданское право: история и современность. — Кн. 1. — С. 755.

на решение данной задачи. Таким образом, право цифровой безопасности представляет собой «срез» отраслей права применительно к проблемам обеспечения цифровой безопасности.

Учебная дисциплина «Право цифровой безопасности» адресована главным образом студентам профиля «Экономическая безопасность» для получения представления о правовых аспектах своей будущей профессиональной деятельности. Поэтому некоторые сложные для понимания специфические юридические проблемы излагаются упрощено.

Очевидно, что начнется процесс становления учебной дисциплины. Идет поиск своего предмета изучения. Очевидно, что он будет представлять собой симбиоз содержания учебных дисциплин право экономической безопасности и цифровое право.

1.5. Обзор основных публикаций по праву цифровой безопасности

Информация о проблемах права цифровой безопасности содержаться в публикациях по многим отраслям законодательства, к важнейшим из которых очевидно относятся цифровое законодательство и законодательное обеспечение экономической безопасности.

Правовые проблемы обеспечения экономической безопасности *в диссертациях*[18] И. А. Аксенова [1], О. С. Белова [2], В. В. Блохина [3], А. П. Герасимова [4], Н. В. Генрих [5], А. П. Горелова [6], В. В. Злобина [7], Ю. В. Игнатова [8], А. А. Козырева [9], Д. В. Кочегина [10], М. А. Кочубея [11], И. Н. Крючковой [12], В. Н. Курочкина [13], И. А. Кутузова [14], Р. Р. Ленковской [15], Е. Н. Лысенковой [16], Е. Н. Майоровой [17], Р. Х. Мусова [18], В. М. Простовой [19], В. И. Сенина [20], К. А. Стрельникова [21], А. В. Сюсюкина [22], С. В. Тимофеева [23], С. А. Тропина [24], А. Х. Хаупшева [25], Д. А. Хрулева [26], С. Ю. Чапчикова [27].

Самыми значимыми *публикациями по цифровому праву* в настоящее время являются диссертации К. А. Мефодьевой[19] (кандидатская) и П. М. Морхата[20] (докторская), а также первый

[18] См. в Списке диссертаций в конце главы.

[19] Мефодьева К. А. Цифровые данные как объект гражданско-правового регулирования в Германии, США и России. Дис. … канд. юрид. наук. — 2019.

[20] Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы. Дис. … д-ра юрид. наук. — М., 2018.

отечественный учебник по цифровому праву, подготовленный коллективом Московского государственного юридического университета и преподавателями ряда других вузов[21].

Имеются также коллективные работы в сфере уголовного, финансового и трудового права и по подотрасли гражданского права — праву интеллектуальной собственности.

Уголовно-правовые аспекты цифровизации рассмотрены в коллективной монографии сотрудников секции публичного права Института законодательства и сравнительного правоведения при Правительстве РФ[22]. Анализ *финансово-правовых проблем цифровизации* содержится в коллективной монографии, подготовленной под редакцией И. А. Цинделиани[23]. Специфика *трудовых правоотношений* рассмотрена в работе под редакцией Ю. П. Орловского и Д. Л. Кузнецова[24].

Из всех подотраслей *гражданского права* внимание уделено цифровым отношениям в праве интеллектуальной собственности[25]. Причем работа сотрудника Высшей школы экономики Е. А. Войниканис была опубликована еще до начала цифровой трансформации в РФ.

К наиболее содержательным статьям[26] по цифровому праву относятся работы следующих авторов:

1) цифровые права (токены): В. К. Андреев [1], Л. Ю. Василевская [2], А. М. Лаптева [3], Л. А. Новоселова [4] и др.;

2) цифровые деньги (криптовалюта): В. С. Белых [5], М. Г. Егорова [6], Л. Г. Ефимова [7], А. А. Максуров [8], Л. А. Новоселова [9], А. И. Савельев [10], Э. Л. Сидоренко [11] и др.;

---

[21] Право цифровой экономики : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — М.: Изд-во «Проспект», 2020.

[22] Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н. А. Голованова и др. — М.: ИЗиСП, Контракт, 2019. — 212 с.

[23] Финансовое право в условиях развития цифровой экономики: монография / К. Т. Анисина и др.; под ред. И. А. Цинделиани. — М.: Изд-во «Проспект», 2019. — 320 с.

[24] Особенности регулирования трудовых отношений в условиях цифровой экономики: монография / И. Я. Белицкая и др.; под ред. Ю. П. Орловского, Д. Л. Кузнецова. — М.: Изд-во «Контракт», 2018. — 152 с.

[25] См. напр.: Энтин В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи). — М.: Изд-во «Статут», 2017; Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. — М.: Изд-во «Юриспруденция», 2013 и др.

[26] См. в Списке статей в конце главы.

3) цифровые платформы (блокчейн): М. В. Мажорина [12], А. А. Максуров [13], А. И. Савельев [14] и др.;

4) смарт-контракты (самоисполняемые сделки): А. И. Савельев [15], Д. В. Федоров [16] и др.;

5) искусственный интеллект (нейросети, роботы, боты): П. М. Морхат [17], А. В. Нестеров [18], Н. Ф. Попова [19] и др.

1.6. Источники правового регулирования

Правовую основу обеспечения цифровой безопасности, так же, как и иных сфер общественных отношений, составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности (ст. 5 ФЗ «О безопасности»).

В настоящее время *словосочетание* «*цифровая безопасность*» *используется только в подзаконных актах*. Так, например, в государственном докладе Роспотребнадзора «Защита прав потребителей в Российской Федерации в 2016 году» говорится том, что цифровая грамотность — это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета. Она включает в себя цифровое потребление, цифровые компетенции и *цифровую безопасность*. В последнем докладе Роспотребнадзора использован термин «кибербезопасность»[27].

В идеале любое правоотношение должно регулироваться одним нормативным актом. Иначе возможна коллизия нормативных актов, то есть ситуация, когда нормативные акты, претендующие на регламентацию одного правоотношения, поразному определяют права и обязанности сторон правоотношения. Это возможно в силу целого ряда объективных и субъективных причин (например, некачественная подготовка проекта нормативного акта).

[27] Защита прав потребителей в Российской Федерации в 2019 году: государственный доклад. — М.: Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека, 2020. — С. 304.

Существуют следующие *правила разрешения коллизий*: (1) иерархия нормативных актов (*иерархическая коллизия*); (2) преимущество специального акта перед общим (*содержательная коллизия*) и (3) преимущество более позднего акта над ранее принятым (*темпоральная коллизия*).

В статье 10 *проекта федерального закона* «*О нормативных правовых актах в Российской Федерации*»[28] следующим образом определена иерархия нормативных правовых актов:

1. Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации.

2. Законы и иные нормативные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.

3. Федеральные законы не могут противоречить федеральным конституционным законам.

4. Нормативные правовые акты Президента Российской Федерации, Совета Федерации и Государственной Думы Федерального Собрания Российской Федерации не должны противоречить федеральным законам.

5. Указы Президента Российской Федерации, восполняющие пробелы в сфере регулирования федеральными законами, не обладают юридической силой федерального закона и действуют до принятия соответствующих федеральных законов.

6. Нормативные правовые акты Правительства Российской Федерации не могут противоречить федеральным законам и указам Президента Российской Федерации.

7. Нормативные правовые акты федеральных органов исполнительной власти не могут противоречить федеральным законам, нормативным правовым актам Президента Российской Федерации и Правительства Российской Федерации.

8. Правительство Российской Федерации вправе отменять нормативные правовые акты федеральных органов исполнительной власти или приостанавливать действие этих актов.

---

[28] См. напр.: Рафалюк Е. Е. Концепция законопроекта «О нормативных правовых актах в Российской Федерации» // Журнал российского права. — 2012. — № 8. — С. 121–125; О проекте Федерального закона «О нормативных правовых актах в Российской Федерации» // Журнал российского права. — 2013. — № 3. — С. 84–99 и др.

9. Конституция (устав) субъекта Российской Федерации и законы субъекта Российской Федерации, принятые на референдуме субъекта Российской Федерации, являются актами высшей юридической силы в системе нормативных правовых актов субъекта Российской Федерации, имеют прямое действие и применяются на всей территории субъекта Российской Федерации.

10. Законы и иные нормативные правовые акты субъектов Российской Федерации не могут противоречить федеральным законам, принятым по предметам ведения Российской Федерации и предметам совместного ведения Российской Федерации и субъектов Российской Федерации.

В случае противоречия между федеральным законом и нормативным правовым актом субъекта Российской Федерации, принятым вне пределов ведения Российской Федерации, совместного ведения Российской Федерации и субъектов Российской Федерации, действует нормативный правовой акт субъекта Российской Федерации.

Законы субъекта Российской Федерации, иные нормативные правовые акты субъекта Российской Федерации не могут противоречить конституции (уставу) субъекта Российской Федерации.

11. Нормативные правовые акты законодательного или представительного органа государственной власти субъекта Российской Федерации не могут противоречить федеральным законам и законам субъекта Российской Федерации.

12. Нормативные правовые акты высшего должностного лица субъекта Российской Федерации не могут противоречить федеральным законам, нормативным правовым актам Президента Российской Федерации и Правительства Российской Федерации, законам субъекта Российской Федерации.

Нормативные правовые акты высшего исполнительного органа государственной власти субъекта Российской Федерации не могут противоречить федеральным законам, нормативным правовым актам Президента Российской Федерации и Правительства Российской Федерации, законам субъекта Российской Федерации, правовым актам высшего должностного лица субъекта Российской Федерации (руководителя высшего исполнительного органа государственной власти субъекта Российской Федерации).

Нормативные правовые акты органов исполнительной власти субъекта Российской Федерации не могут противоречить федеральным законам, нормативным правовым актам Президента Российской Федерации и Правительства Российской Федерации, законам субъекта Российской Федерации, правовым актам высшего должностного лица субъекта Российской Федерации (руководителя высшего исполнительного органа государственной власти субъекта Российской Федерации) и высшего исполнительного органа государственной власти субъекта Российской Федерации.

13. Муниципальные нормативные правовые акты не должны противоречить федеральным законам и иным нормативным правовым актам Российской Федерации, а также конституциям (уставам), законам, иным нормативным правовым актам субъектов Российской Федерации.

Устав муниципального образования и оформленные в виде нормативных правовых актов решения, принятые на местном референдуме (сходе граждан), являются актами высшей юридической силы в системе муниципальных нормативных правовых актов, имеют прямое действие и применяются на всей территории муниципального образования. Иные муниципальные нормативные правовые акты не должны противоречить уставу муниципального образования и правовым актам, принятым на местном референдуме (сходе граждан).

Нормативные правовые акты главы муниципального образования, главы местной администрации, иных органов местного самоуправления и должностных лиц местного самоуправления, предусмотренных уставом муниципального образования, не должны противоречить нормативным правовым актам представительного органа муниципального образования.

14. Юридическая сила производного и вспомогательного нормативного правового акта соответствует юридической силе основного нормативного правового акта[29].

Темпоральная коллизия разрешается с помощью правила «lex posterior derogat legi prior» («позднейшим законом отменяется более ранний»). Наиболее важным это правило является при применении советских актов. Законы и иные нормативные

[29] https://docs.cntd.ru/document/420243605

правовые акты, принятые правотворческими органами бывшего Союза ССР, РСФСР, иными правотворческими органами, прекратившими впоследствии свое существование, применяются на территории Российской Федерации в части, не противоречащей Конституции Российской Федерации, международным договорам Российской Федерации, федеральным конституционным законам, федеральным законам и иным нормативным правовым актам Российской Федерации, до принятия соответствующих законов и иных нормативных правовых актов (Закон РСФСР от 24.10.1990 г. «О действии актов органов Союза ССР на территории РСФСР»).

Все правовые нормы, в том числе и в сфере цифровых правоотношений, являются обязательными. Но по *характеру своего действия* они подразделяются на императивные, диспозитивные и факультативные. При разработке нормативных актов в сфере цифровых отношений законодатель наиболее часто использует императивные и диспозитивные нормы.

Императивные нормы устанавливают определенное правило поведения, которое не может быть изменено соглашением сторон. Например, согласно пункту 5 статьи 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», к правоотношениям, возникающим при выпуске, учете и обращении цифровых финансовых активов, в том числе с участием иностранных лиц, применяется российское право.

Диспозитивные нормы устанавливают правило, содержание которого может быть изменено соглашением сторон. Например, согласно пункту 4 статьи 4 вышеуказанного нормативного акта, записи о цифровых финансовых активах не погашаются в случае, если обладателем цифровых финансовых активов становится лицо, их выпустившее, *если иное* не предусмотрено решением о выпуске цифровых финансовых активов.

Другой пример. *Если иное не предусмотрено условиями пользовательского или иного соглашения* потребителя с владельцем агрегатора, уведомление продавцу об отказе от исполнения договора купли-продажи (договора возмездного оказания услуг) может быть направлено владельцу агрегатора,

который обязан направить его продавцу (п. 2.2 ст. 12 Закона РФ от 7 февраля 1992 г., ред. от 22 декабря 2020 г. «О защите прав потребителей»).

Таким образом, внешним признаком диспозитивной нормы, как правило, является наличие оговорки «если иное не предусмотрено сторонами правоотношения».

Факультативные нормы применяются к правоотношению только в том случае, если на это есть прямое согласие сторон. Существует также и практика наделения решениями судов отмененных актов качеством факультативных норм.

Таким образом, *императивные нормы применяются преимущественно перед условиями договора*, *диспозитивные — только в том случае*, *если стороны не указали в договоре иное*, *факультативные — если в договоре содержится на них ссылка*.

Конституция РФ имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции РФ (статья 15).

Конституция РФ содержит принципиальные положения, устанавливающие невозможность сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (статья 24), гарантию свободы слова и мысли, свободы литературного, художественного, научного, технического и других видов творчества; гарантию свободы совести, включая право распространять религиозные и иные убеждения (статья 28), право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом (статья 29) и т. д.

В результате всенародного голосования, состоявшегося 1 июля 2020 года, в Конституцию РФ включены еще две нормы, согласно которым к ведению Российской Федерации отнесены *информация*, *информационные технологии* и связь (пункт «и» статьи 71) и необходимость обеспечения безопасности личности, общества и государства при применении *информационных технологий*, *обороте цифровых данных* (пункт «м» статьи 71).

Основной закон закрепляет *экономической основы конституционного строя*: (1) единое экономическое пространство; (2) свободное перемещение товаров, услуг и финансовых средств; (3) поддержка конкуренции; (4) свобода экономической

деятельности; (5) признание равенства частной, государственной, муниципальной и иных форм собственности, в том числе на землю и другие природные ресурсы; (6) защита частной, государственной, муниципальной и иных форм собственности и др. (ст. 8 и 9 Конституции РФ).

Ряд конституционных норм действуют в сфере обеспечения безопасности, в том числе и экономической (например, п. 3 ст. 37, п. 1 ст. 72, п. 2 ст. 74 Конституции РФ и др.).

Судебно-правовую охрану Конституции РФ производит *Конституционный Суд РФ*. Важнейший функцией Конституционного Суда РФ является то, что он разрешает следующие дела о соответствии Конституции РФ:

1) нормативных актов федеральных органов (федеральных законов, нормативных актов Президента РФ, Совета Федерации, Государственной Думы и Правительства РФ);

2) актов субъектов РФ (конституций республик, уставов, а также законов и иных нормативных актов субъектов Российской Федерации, изданных по вопросам, относящимся к ведению органов государственной власти Российской Федерации и совместному ведению органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации);

3) договоров между органами государственной власти Российской Федерации и органами государственной власти субъектов Российской Федерации, договоров между органами государственной власти субъектов Российской Федерации;

4) не вступивших в силу международных договоров Российской Федерации[30].

Конституционный Суд РФ может отменить действующие нормы права, обязать законодателя в установленный срок внести изменения в правовые нормы или установить новые правовые нормы. Его решения обязательны на всей территории Российской Федерации для всех представительных, исполнительных и судебных органов государственной власти, органов местного самоуправления, предприятий, учреждений, организаций, должностных лиц, граждан и их объединений.

---

[30] ФКЗ от 21 июля 1994 г. (ред. от 9 ноября 2020 г.) «О Конституционном Суде Российской Федерации» // Собрание законодательства РФ, 1994. — № 13. — Ст. 1447.

В настоящее время существует обширная практика *Конституционного Суда РФ* по проблемам информационных отношений[31], обеспечения экономической безопасности государства[32], экономической безопасности банковской деятельности[33] и т. д.

Международным договором именуется соглашение, заключенное между государствами в письменной форме и регулируемое международным правом, независимо от того, содержится ли такое соглашение в одном документе, в двух или нескольких связанных между собой документах, а также независимо от его конкретного наименования (статья 2 Закона РФ «О международных договорах РФ» от 21 июля 1995 г.).

Согласно пункту 4 статьи 15 Конституции РФ, *общепризнанные принципы и нормы международного права и международные договоры РФ* являются составной частью правовой системы Российской Федерации.

Данное обстоятельство означает, что *отношения в сфере обеспечения экономической безопасности регулируются совместно международно-правовыми и внутригосударственными актами* (*как российскими*, *так и иностранными*). Положения официально опубликованных международных договоров РФ действуют непосредственно (ч. 3 ст. 5 ФЗ «О международных договорах Российской Федерации»).

В результате общероссийского голосования 1 июля 2020 года в Конституцию РФ были внесены дополнения в части исполнения решений международных судов. Согласно статье 79 Конституции РФ, решения межгосударственных органов, принятые на основании положений международных договоров

---

[31] Постановление Конституционного Суда РФ от 26 октября 2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона “Об информации, информационных технологиях и о защите информации” в связи с жалобой гражданина А. И. Сушкова» // Собрание законодательства РФ, 2017. — № 45. — Ст. 6735.

[32] См. напр.: постановление Конституционного Суда РФ от 13 февраля 2018 г. № 8-П «По делу о проверке конституционности положений пункта 4 статьи 1252, статьи 1487 и пунктов 1, 2 и 4 статьи 1515 Гражданского кодекса Российской Федерации в связи с жалобой общества с ограниченной ответственностью “ПАГ”»; постановления Конституционного Суда РФ от 14 мая 2013 г. № 9-П, от 26 ноября 2012 № 28-П, от 17 ноября 2011 г. № 1621-О-О, от 7 июня 2011 г. № 805-О и др.

[33] Например, постановление Конституционного Суда РФ от 27 октября 2015 г. № 28-П.

Российской Федерации *в их истолковании*, *противоречащем Конституции Российской Федерации*, не подлежат исполнению в Российской Федерации.

Причиной включения в Конституцию РФ статьи 79 является то, что Европейский Суд по правам человека начал в одностороннем порядке расширительно толковать нормы о своих полномочиях и принимать решения, касающиеся традиционных для российского народа семейных ценностей, противоречащие основам публичного правопорядка Российской Федерации.

Следует также учитывать, что из трех разновидностей международных договоров — *межгосударственных*, *межправительственных и межведомственных* — преимуществом перед законами, по общему правилу, обладают только межгосударственные.

РФ участвует в ряде договоров как государство-продолжатель СССР. Такое понятие является новым в международном праве, так как обычно в подобных обстоятельствах применяется термин «правопреемник». Но правопреемство не распространяется на членство в международных организациях, а СССР являлся постоянным членом Совета Безопасности. По взаимному соглашению государств за РФ был признан статус «государства-продолжателя, что означает принятие всех прав и обязанностей СССР (за исключением тех обязательств, которые были неразрывно связаны с территорией другого члена СНГ).

Специальных международных договоров в сфере обеспечения экономической безопасности не существуют, но эти нормы содержатся в большом количестве международно-правовых актов, важнейшими из которых являются акты главных органов Организации Объединенных Наций — Генеральной ассамблеи, Совета Безопасности, Экономического и Социального Совета и Международного Суда.

Генеральная ассамблея — главный совещательный, директивный и представительный орган Организации Объединенных Наций и состоит из всех членов Организации. Акты Ассамблеи не являются обязательными, но она обладает большим авторитетом.

В сфере обеспечения экономической безопасности приняты следующие документы: Хартия экономических прав и обя-

занностей государств (принята 12 декабря 1974 г. Резолюцией 3281 (XXIX) на 2315-ом пленарном заседании 29-ой сессии Генеральной Ассамблеи ООН)[34], Декларация о запрещении применения военного, политического или экономического принуждения при заключении международных договоров (принята 23 мая 1969 г. конференцией ООН по праву договоров)[35], Руководящие принципы для защиты интересов потребителей (приняты 9 апреля 1985 г. Резолюцией 39/248 на 106-м пленарном заседании Генеральной Ассамблеи ООН), Декларация Организации Объединенных Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях (принята 16 декабря 1996 г. Резолюцией 51/191 на 86-м пленарном заседании Генеральной Ассамблеи ООН) и др.

22 августа 2012 г. РФ стала членом *Всемирной торговой организации*[36]. При этом РФ приняла на себя ряд обязательств закрепленных, в частности, в Протоколе о присоединении Российской Федерации к Марракешскому соглашению об учреждении Всемирной торговой организации (16 декабря 2011 г.).

Российская Федерация является членом *Евразийского экономического союза* (*ЕАЭС*). Договор о Евразийском экономическом союзе подписан 29 мая 2014 г., с изменениями вступил в силу с 12 августа 2017 г.

Членами Евразийского экономического сообщества, кроме РФ, в настоящее время являются Армения, Беларусь, Казахстан и Кыргызстан. Основными целями Союза являются: (1) создание условий для стабильного развития экономик государств-членов в интересах повышения жизненного уровня их населения; (2) стремление к формированию единого рынка товаров, услуг, капитала и трудовых ресурсов в рамках Союза и (3) всесторонняя модернизация, кооперация и повышение конкурентоспособности национальных экономик в условиях глобальной экономики.

---

[34] Действующее международное право. В 3-х т. — М.: Московский независимый институт международного права, 1997. — Т. 3. — С. 135–145.

[35] Международное право. Сборник документов. — М.: Юридическая литература, 2000. — С. 106.

[36] ФЗ от 21 июля 2012 г. «О ратификации Протокола о присоединении Российской Федерации к Марракешскому соглашению об учреждении Всемирной торговой организации от 15 апреля 1994 г.» // Собрание законодательства РФ, 2012. — № 37. — Ст. 4986.

Согласно Консультативному заключению Экономического Суда СНГ, акты ЕврАзЭС — предшественника ЕАЭС — так же, как и акты любой международной организации, подразделяются на две группы: по внутриорганизационным вопросам (*внутренняя регламентация*) и по вопросам непосредственного осуществления целей международной организации (*внешняя регламентация*).

Первая группа актов касается принятия правил процедуры, правил персонала и установления иных норм, регулирующих деятельность внутри международной организации. К ним относятся решения органов ЕврАзЭС, определяющие структуру и механизм функционирования органов ЕврАзЭС, взаимоотношения между ними, порядок назначения, статус должностных лиц и служащих органов ЕврАзЭС и другие внутриорганизационные вопросы.

Во вторую группу входят акты по вопросам непосредственного осуществления целей международной организации, адресованные государствам-членам и устанавливающие права и обязанности в их взаимоотношениях друг с другом, с третьими государствами и международными организациями[37]. Очевидно, что все эти признаки характерны и для актов ЕАЭС.

К важнейшим общим международным договорам *в сфере цифровых отношений* относится *Устав Международного союза электросвязи* от 22 декабря 1992 года. Согласно этому документу, государства обязаны обеспечить передачу сообщений от населения при помощи международной службы общественной корреспонденции с предоставлением по каждой категории корреспонденции одинаковых условий обслуживания, тарифов и гарантий без предоставления какого-либо приоритета или предпочтений.

Из декларативных документов важнейшим является *Окинавская хартия глобального информационного общества*, принятая на совещании стран восьмерки 22 июля 2000 года. Данный документ содержит следующие правила, устанавливающие необ-

[37] Консультативное заключение Экономического Суда СНГ от 10 марта 2006 г. № 01-1/3-05 «По запросу Интеграционного Комитета Евразийского экономического сообщества о толковании части второй статьи 1, части первой статьи 14 Договора об учреждении Евразийского экономического сообщества от 10 октября 2000 года» // ИПБ «Гарант».

ходимость ликвидации обособления стран в области информации и знаний (цифрового разрыва):

– принцип содействия развития конкуренции в телекоммуникационной сфере;

– защита прав интеллектуальной собственности на информационные технологии;

– развитие трансграничной электронной торговли в контексте жестких рамок Всемирной торговой организации;

– продолжение практики освобождения электронных переводов от таможенных пошлин до тех пор, пока она не будет рассмотрена вновь на следующей министерской конференции Всемирной торговой организации;

– развитие механизма защиты частной жизни потребителя, электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

Растет значение актов, принятых в рамках *Евразийского экономического союза*[38].

К ним, в частности, относятся следующие программные документы:

– Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года, утвержденный решением Высшего Евразийского экономического совета от 11 октября 2017 г. № 12.

– О механизмах реализации проектов в рамках цифровой повестки Евразийского экономического союза, утвержденный решением Евразийского межправительственного совета от 1 февраля 2019 г. № 1.

– О формате и структуре предоставления информации об инициативе в рамках реализации цифровой повестки Евразийского экономического союза, утвержденный решением Коллегии Евразийской экономической комиссии от 19 февраля 2018 г. № 29.

[38] Евразийский экономический союз — международная организация региональной экономической интеграции. Входят Армения, Беларусь, Казахстан, Киргизия и Россия. В ЕАЭС обеспечивается свобода движения товаров, услуг, капитала и рабочей силы, а также проведение скоординированной, согласованной или единой экономической политики в целях всесторонней модернизации, кооперации и повышения конкурентоспособности национальных экономик в интересах повышения жизненного уровня государств-членов.

Кроме международных договоров важное значение для регулирования экономических отношений имеет *практика международных судебных учреждений*. В частности, РФ является участником Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. (в ред. от 11 мая 1994 г.)[39]. Соответственно она обязана руководствоваться практикой Европейского Суда по правам человека по вопросам толкования и применения данной Конвенции и протоколов к ней[40].

Суд Евразийского экономического сообщества рассматривает споры не только членов данного сообщества, но и членов Таможенного Союза. Согласно статье 13 Статута Суда Евразийского экономического сообщества от 5 июля 2010 г.[41], юрисдикционное учреждение (1) обеспечивает единообразное применение международных договоров и принимаемых органами ЕАЭС решений; (2) рассматривает споры экономического характера, возникающие между членами организации по вопросам реализации решений органов ЕАЭС и положений договоров, действующих в рамках ЕАЭС и (3) осуществляет толкование положений международных договоров, действующих в рамках ЕАЭС, и решений органов ЕАЭС.

Федеральные законы. Закон является актом принятым высшим органом государственной власти. Порядок вступления в силу федеральных законов в настоящее время регулируется федеральным законом от 14 июня 1994 г. (ред. от 1 мая 2019 г.) «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания».

Основным законом является ФЗ от 28 декабря 2010 г. (ред. от 9 ноября 2020 г.) «О безопасности». Он определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов

---

[39] Бюллетень международных договоров. — 2001. — № 3. — С. 3–44.

[40] Канашевский В. А. Международное частное право. — М.: Изд-во «Международные отношения», 2019. — С. 58.

[41] Собрание законодательства РФ, 2011. — № 38. — Ст. 5322.

Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.

Серьезным *недостатком ФЗ «О безопасности» является отсутствие определения понятия «безопасность»*. В качестве предмета регулирования указаны: (1) основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации и (2) полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности. В силу того, что три главы из четырех ФЗ «О безопасности» содержат нормы о статусе субъектов, обеспечивающих безопасность, он представляет собой *не закон о безопасности*, *а закон об органах*, *обеспечивающих безопасность*. Поэтому при применении ФЗ «О безопасности» необходимо руководствоваться доктринальным определением безопасности[42]. Частным случаем данной проблемы является *отсутствие легитимного перечня видов безопасности*[43] и, соответственно, «умножение объектов безопасности и элементов ее состава, а также выхолащивание ее подлинного содержания при акценте на множественность опасностей»[44].

---

[42] См. напр.: Дворядкина Е. Б. Национальная экономика. В 2-х кн. — Екатеринбург, 2001. — Кн. 1. — С. 75.

[43] В литературе предпринимаются попытки восполнить данный пробел путем составления исчерпывающего перечня видов безопасности. Так, например, по мнению Е. С. Калины, к ним относятся государственная безопасность, международная безопасность, экономическая безопасность, общественная безопасность, оборонная безопасность, информационная безопасность, экологическая безопасность, национальная безопасность, военная безопасность, энергетическая безопасность, безопасность труда, безопасность дорожного движения, ядерная и радиационная безопасность, безопасность малого города и региональная безопасность (Калина Е. С. Понятие безопасности и право на безопасность как одно из личных прав // Научные труды. Российская академия юридических наук. В 3 т. — М.: Издат. группа «Юрист», 2004. — Вып. 4. — Т. 1. — С. 359–361).

[44] Колокольцев В. А. Обеспечение государственных интересов России в контексте концепции национальной безопасности: автореф. дис. … д-ра юрид. наук. — СПб., 2005. — С. 28.

Предполагалось принятие *Федерального закона* «*Об экономической безопасности Российской Федерации*»[45]. «Важнейшей задачей совершенствования правового регулирования экономической безопасности является принятие закона «Об экономической безопасности Российской Федерации». Этот закон должен содержать основные понятия экономической безопасности; механизм ее обеспечения; перечень критериев, показателей, количественных (пороговых) параметров. Здесь же важно предусмотреть механизм и порядок экспертизы и оценки федеральных законов, указов, постановлений Президента и Правительства с точки зрения их соответствия национальным интересам в области экономики и собственно экономической безопасности Российской Федерации»[46]. Но этот акт был предложен в период обострения противостояния с западными странами и поэтому был слишком политизированным. Так, в частности, законопроект содержал прямой запрет на использование иностранных кредитов для финансирования расходов федерального бюджета Российской Федерации и вводился мораторий на обслуживание платежей по внешней задолженности Российской Федерации перед странами НАТО. Правительство РФ в своем заключении на данный документ указало на нецелесообразность его принятия[47].

В настоящее время термин «*экономическая безопасность*» *содержится в следующих 10 федеральных законах*:

1. Часть 1 статьи 281 Уголовного кодекса РФ «Диверсия» (совершение взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий, сооружений, объектов транспортной инфраструктуры и транспортных средств, средств связи, объектов жизнеобеспечения населения в целях подрыва *экономической безопасности*).

2. Пункт 1 статьи 3 Закона РФ от 27 ноября 1992 г. (ред. от 30 декабря 2020 г.) «Об организации страхового дела в Рос-

---

[45] Собрание законодательства РФ, 1996. — № 34. — Ст. 4059.

[46] Батова В. Н., Малахова М. Н. Проблемы административно-правового регулирования экономической безопасности в Российской Федерации // XXI век: итоги прошлого и проблемы настоящего. — 2014. — № 2 (18). — С. 143.

[47] Заключение Правительства РФ от 11 мая 1999 г. № 2116п-П5 «На проект Федерального закона “Об обеспечении экономической безопасности Российской Федерации”» // ИПБ «Консультант-плюс».

сийской Федерации» (задачами организации страхового дела являются …установление принципов страхования и формирование механизмов страхования, обеспечивающих *экономическую безопасность* граждан и хозяйствующих субъектов на территории Российской Федерации).

3. Пункт 1 статьи 1 ФЗ от 27 ноября 2010 г. (ред. от 24 февраля 2021 г.) «О таможенном регулировании в Российской Федерации» (целями настоящего Федерального закона являются: …обеспечение *экономической безопасности* Российской Федерации при осуществлении внешней торговли товарами).

4. Пункт 1 статьи 19 ФЗ от 21 июля 1997 г. (ред. от 31 июля 2020 г.) «О службе в таможенных органах Российской Федерации» (гражданин, принятый на службу в таможенные органы, не позднее двух месяцев со дня присвоения ему первого специального звания принимает присягу: клянусь при осуществлении полномочий сотрудника таможенного органа Российской Федерации …защищать экономический суверенитет и *экономическую безопасность* Российской Федерации, добросовестно исполнять свои должностные обязанности).

5. Пункт 1 статьи 6 ФЗ от 23 июня 2016 г. «Об основах системы профилактики правонарушений в Российской Федерации» (профилактика правонарушений осуществляется по следующим основным направлениям: …обеспечение *экономической безопасности*).

6. Пункт 1 статьи 1 ФЗ от 26 июня 2008 г. (ред. от 8 февраля 2020 г.) «Об обеспечении единства измерений» (целями настоящего Федерального закона являются: …обеспечение потребности граждан, общества и государства в получении объективных, достоверных и сопоставимых результатов измерений, используемых в целях защиты жизни и здоровья граждан, охраны окружающей среды, животного и растительного мира, обеспечения обороны и безопасности государства, в том числе *экономической безопасности*).

7. Пункт 2 статьи 2 ФЗ от 13 декабря 1994 г. (ред. от 13 июля 2015 г.) «О поставках продукции для федеральных государственных нужд» (при разработке федеральных целевых программ необходимо предусматривать …комплексность и *экономическую безопасность* разрабатываемых мероприятий).

8. Статья 2 ФЗ от 20 ноября 1999 г. «Об участках недр, право пользования которыми может быть предоставлено на условиях раздела продукции (участке недр “Северные территории”)», статья 2 ФЗ от 20 ноября 1999 г. «Об участках недр, право пользования которыми может быть предоставлено на условиях раздела продукции (Приобском (северном лицензионном участке) нефтяном месторождении)» и статья 2 ФЗ от 31 мая 1999 г. «Об участках недр, право пользования которыми может быть предоставлено на условиях раздела продукции (Лугинецком, Федоровском и других нефтегазоконденсатных месторождениях)» (в интересах *экономической безопасности* Российской Федерации переговоры и заключение соглашений о поисках, разведке и добыче минерального сырья на условиях раздела продукции в отношении участка недр …по совместному решению Правительства Российской Федерации и органа исполнительной власти Ненецкого автономного округа без проведения конкурсов и аукционов осуществляются или с юридическими лицами, являющимися пользователями указанного участка недр, или с созданными с участием пользователей указанного участка недр юридическими лицами, или с созданными с участием пользователей указанного участка недр объединениями юридических лиц).

Важнейшим нормативным актом в сфере цифровых технологий является федеральный закон от 27 июля 2006 г. (ред. от 8 июня 2020 г.) «Об информации, информационных технологиях и о защите информации». Данный документ регулирует отношения, возникающие при (1) реализации права на поиск, получение, передачу, производство и распространение информации; (2) применении информационных технологий и (3) обеспечении защиты информации.

Принято считать, что *базовыми законами в сфере цифровизации* являются федеральный закон «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса РФ», федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» и федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Федеральный закон № 424632-7 «*О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации*», именуемый также законом цифровых правах, создает основу для регулирования отношений в рамках цифровой экономики. Он вступил в силу 1 октября 2019 года. Этим документом закрепляется понятие «цифровые права»[48] путем включения в Гражданского кодекса РФ статьи 141^1. Согласно пункту 1 данной статьи, *цифровыми правами* признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия, осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Особенностью этих прав является то, что осуществление, распоряжение, в том числе передача, залог, обременение права цифровой экономики другими способами или ограничение распоряжения ими возможны только в информационной системе без обращения к третьему лицу.

Законом вводятся также *смарт-контракты*, обычно именуемые самоисполняемыми сделками. Но, согласно вышеуказанному нормативному акту, смарт-контракт не является отдельной сделкой, это лишь условие об автоматическом исполнении любого гражданско-правового договора (договора комиссии, подряда, перевозки и др.).

Данным документом также решен вопрос о легализации сбора и обработки *значительных массивов обезличенной информации* (в обиходе — «Big data»). Для этого в статью 783.1 Гражданского кодекса РФ была включена конструкция договора об оказании услуг по предоставлению информации. При этом было указано, что договором может предусматриваться обязанность не совершать действия, в результате которых передаваемая информация может быть раскрыта третьим лицам.

Федеральный закон «*О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации*» принят 22 июля 2020 года и вступил в силу 1 января 2021 года. Согласно статье 2 законопроекта, под *цифровым финансовым активом* понимаются

[48] Широко используемый экономистами термин «токен», используемый как синоним цифрового права, в окончательной редакции данного нормативного акта отсутствует.

цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые закреплены в решении о выпуске цифровых финансовых активов.

Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» принят 2 августа 2019 года и вступил в силу 1 января 2020 года. Предметом данного документа являются отношения по привлечению инвестиций субъектами предпринимательской деятельности посредством инвестиционных платформ, а также деятельность операторов инвестиционных платформ по организации розничного финансирования.

Федеральный закон от 31 июля 2020 г. «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (закон о «регуляторных песочницах»). Использование регулятивных песочниц обусловлена необходимостью внедрения инноваций в сфере финансовых технологий без риска быть привлеченным к ответственности за потенциальную возможность нарушения действующего законодательства. В случае удачного результата эксперимента содержание законодательства адаптируется к экспериментально выявленным технологиям проведения тех или иных операций: положения программы экспериментального правового режима, устанавливающие условия экспериментального правового режима, могут исключать или изменять действие положений федерального закона в случае, если это прямо предусмотрено соответствующим федеральным законом (п. 3 статьи 5).

Подзаконные акты принимаются органами исполнительной власти и поэтому они не могут противоречить законам. Их задачей является более подробная регламентация норм, содержащихся в законах.

К подзаконным актам относятся указы Президента, постановления и распоряжения правительства, инструкции, распоряжения и приказы министерств и ведомств. Правовой статус данных документов определен указом Президента РФ от 23 мая 1996 г. (ред. от 29 мая 2017 г.) № 763 «О порядке опубликова-

ния и вступления в силу актов Президента РФ и нормативных актов органов исполнительной власти».

По общему положению, все они должны быть опубликованы, кроме актов или отдельных их положений, содержащих сведения, составляющие государственную тайну, или сведения конфиденциального характера.

Нормативные правовые акты федеральных органов исполнительной власти вступают в силу одновременно на всей территории РФ по истечении десяти дней после дня их официального опубликования, если самими актами не установлен другой порядок вступления их в силу.

Принципиальные положения процесса цифровизации экономики закреплены в настоящее время следующими подзаконными актами:

– Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

– Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента РФ от 13 мая 2017 г. № 208.

– Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

– Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 № 646.

– Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержденный президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16.

Вышеуказанными документами установлено, в частности, следующее:

1. Основной целью является создание экосистемы цифровой экономики Российской Федерации, в которой *данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности* и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

2. *Основными цифровыми технологиями* являются (1) большие данные; (2) нейротехнологии и искусственный интеллект; (3) системы распределенного реестра; (4) квантовые технологии; (5) новые производственные технологии; (6) промышленный Интернет; (7) компоненты робототехники и сенсорика; (8) технологии беспроводной связи и (9) технологии виртуальной и дополненной реальностей.

3. Необходимость создания системы правового регулирования цифровой экономики, основанного на гибком подходе в каждой сфере, а также внедрение гражданского оборота на базе цифровых технологий. Что обуславливает необходимость изменения не только материального, но и процессуального законодательства. В частности, унификация правил подачи в суд документов в электронной форме для арбитражных судов и судов общей юрисдикции.

Акты негосударственного регулирования. Системой важнейших подобных источников регулирования является так называемый lex electronica (lex informatica) — свод транснациональных правовых норм и торговых обычаев, применимых к сделкам в сфере трансграничной электронной торговли, созданный ее участниками для внутреннего пользования и применяемый арбитрами для урегулирования споров на основании намерений сторон и функционального сравнительно-правового анализа с учетом текущего состояния дел в сфере электронной торговли. Концепция «lex electronica» в этой связи рассматривается как «естественное продолжение lex mercatoria», правовое регламентирование торговых операций, совершаемых в электронной среде, в частности с помощью установления норм частной торговли[49].

Нормативные акты Президента РФ и федеральных органов исполнительной власти. Акты Президента РФ и федеральных органов исполнительной власти являются подзаконными и, соответственно, не могут противоречить федеральным законам. Порядок принятия федеральных подзаконных актов определен указом Президента РФ № 763 от 23 мая 1996 г. (в ред. от 29 мая

[49] Казаченок С. Ю. Развитие lex electronica как предпосылка включения в арбитражное соглашение условия об онлайн-арбитраже // Современное право. — 2014. — № 10. — С. 124–130.

2017 г.) «О порядке опубликования и вступления в силу актов Президента РФ и нормативных актов органов исполнительной власти»[50].

Нормативные правовые акты федеральных органов исполнительной власти вступают в силу одновременно на всей территории РФ по истечении десяти дней после дня их официального опубликования, если самими актами не установлен другой порядок вступления их в силу.

Правила подготовки нормативных правовых актов федеральных органов исполнительной и их государственной регистрации утвержденные постановлением Правительства РФ от 13 августа 1997 г. (в ред. от 31 июля 2017 г.) № 1009[51] устанавливают требования к подзаконным актам федерального уровня. Кроме того, в настоящее время необходимо руководствоваться Разъяснениями о применении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации, утвержденными приказом МЮ РФ от 4 мая 2007 г. (в ред. от 26 мая 2009 г.) № 88[52].

Вышеуказанными документами установлен замкнутый перечень нормативных актов, принимаемых высшими исполнительными органами. Теперь они могут приниматься только в форме *постановлений*, *приказов*, *распоряжений*, *правил*, *инструкций* и *положений*. Издание нормативных правовых актов в виде *писем* и *телеграмм* не допускается (п. 2 постановления Правительства РФ № 1009 от 13 августа 1997 г., ред. от 31 июля 2017 г.).

Акты, изданные в ином виде (например, *директивы* и др.), не должны иметь нормативный правовой характер (п. 3 приказа МЮ РФ от 4 мая 2007 г. № 88).

К важнейшим *актам Президента РФ в сфере обеспечения экономической безопасности* относятся:

– Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»[53].

---

[50] Собрание законодательства РФ, 1996. — № 22. — Ст. 2663; 2017. — № 23. — Ст. 3310.

[51] Собрание законодательства РФ, 1997. — № 33. — Ст. 3895.

[52] Бюллетень нормативных актов министерств и ведомств, 2007. — № 23.

[53] Собрание законодательства РФ, 2017. — № 20. — Ст. 2902.

– Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»[54].

– Указ Президента РФ от 1 января 2016 г. № 1 (ред. от 1 июля 2016 г.) «О мерах по обеспечению экономической безопасности и национальных интересов Российской Федерации при осуществлении международных транзитных перевозок грузов с территории Украины на территорию Республики Казахстан или Киргизской Республики через территорию Российской Федерации»[55] и др.

К важнейшим актам Президента РФ в сфере обеспечения экономической безопасности также относятся *стратегии развития отдельных отраслей национальной экономики*:

– Распоряжение Правительства РФ от 15 сентября 2017 г. № 1966-р «Об утверждении Стратегии развития янтарной отрасли Российской Федерации на период до 2025 года»[56].

– Распоряжение Правительства РФ от 17 августа 2017 г. № 1756-р «Об утверждении Стратегии развития транспортного машиностроения Российской Федерации на период до 2030 года»[57].

– Распоряжение Правительства РФ от 28 декабря 2012 г. № 2575-р (ред. от 7 августа 2017 г.) «О Стратегии развития таможенной службы Российской Федерации до 2020 года»[58].

– Постановление Правительства РФ от 1 января 2016 г. № 1 (ред. от 1 августа 2016 г.) «О мерах по реализации Указа Президента Российской Федерации от 1 января 2016 г. № 1 “О мерах по обеспечению экономической безопасности и национальных интересов Российской Федерации при осуществлении международных транзитных перевозок грузов с территории Украины на территорию Республики Казахстан или Киргизской Республики через территорию Российской Федерации”»[59].

Согласно пункту 1 статьи 15 ФЗ от 28 июня 2014 г. (ред. от 3 июля 2016 г.) «О стратегическом планировании в Россий-

---

[54] Собрание законодательства РФ, 2016. — № 1 (ч. II). — Ст. 212.
[55] Там же. — Ст. 215.
[56] Собрание законодательства РФ, 2017. — № 39. — Ст. 5715.
[57] Там же. — № 34. — Ст. 5323.
[58] Собрание законодательства РФ, 2013. — № 2. — Ст. 109.
[59] Собрание законодательства РФ, 2016. — № 2 (ч. I). — Ст. 408.

ской Федерации»[60], *ежегодное послание Президента Российской Федерации Федеральному Собранию Российской Федерации о положении в стране и об основных направлениях внутренней и внешней политики государства* является основой для определения стратегических целей и приоритетов социально-экономического развития и обеспечения национальной безопасности Российской Федерации, определения направления достижения указанных целей, важнейших задач, подлежащих решению, а также для разработки других документов стратегического планирования.

Первым таким документом было Послание Президента РФ Федеральному Собранию от 24 февраля 1994 г. «Об укреплении Российского государства (Основные направления внутренней и внешней политики)»[61], последним, тринадцатым — послание от 1 декабря 2016 года.

Во исполнение ежегодного послания Президент Российской Федерации издает *указы*, в которых определяются стратегические цели и приоритеты социально-экономического развития и обеспечения национальной безопасности Российской Федерации, направления достижения указанных целей и решения важнейших задач в сфере социально-экономического развития и обеспечения национальной безопасности Российской Федерации, а также документы стратегического планирования, подлежащие разработке. К ним, в частности, относятся Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»[62], Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии и мерах по обеспечению экономической безопасности и национальных интересов Российской Федерации при осуществлении международных транзитных перевозок грузов с территории Украины на территорию Республики Казахстан или Киргизской Республики через территорию Российской Федерации»[63] и др.

Указы Президента РФ детализируются *постановлениями Правительства РФ и ведомственными актами*. Например, постановление Правительства РФ от 1 января 2016 г. № 1 (ред. от 1 августа 2016 г.) «О мерах по реализации Указа Президента

---

[60] Собрание законодательства РФ, 2014. — № 26 (ч. I). — Ст. 3378.
[61] Российская газета, 25.02.1994.
[62] Собрание законодательства РФ, 2016. — № 1 (ч. II). — Ст. 12.
[63] Там же. — Ст. 215.

Российской Федерации от 1 января 2016 г. № 1 “О мерах по обеспечению экономической безопасности и национальных интересов Российской Федерации при осуществлении международных транзитных перевозок грузов с территории Украины на территорию Республики Казахстан или Киргизской Республики через территорию Российской Федерации”»[64], Распоряжение Правительства РФ от 6 октября 2011 г. № 1757-р (ред. от 26 декабря 2014 г.) «Об утверждении Стратегии социально-экономического развития Уральского федерального округа до 2020 года», приказ Минпромторга России от 22 февраля 2011 г. № 206 «Об утверждении Стратегии развития энергомашиностроения Российской Федерации на 2010–2020 годы и на перспективу до 2030 года» и др.

Акты высших судебных органов. Правовая природа норм судебных органов продолжает оставаться предметом дискуссий. Принято считать, что судебные решения являются источниками права только в странах англосаксонской системы права. Россия относится к странам романо-германской системы, и поэтому сказанное для нас не характерно. В обоснование данного вывода ссылаются на статью 120 Конституции РФ, согласно которой судьи независимы и подчиняются только Конституции РФ и федеральному закону, и поэтому разъяснения высших судебных органов по вопросам применения действующего законодательства не могут быть обязательными для судов при рассмотрении ими конкретных дел.

Однако статья 126 Конституции РФ предоставляет Верховному Суду РФ полномочия на дачу разъяснений по вопросам судебной практики. Следует также учитывать указание, содержащееся в пункте 4 постановления Пленума Верховного Суда РФ от 19 декабря 2003 г. № 23 «О судебном решении», о необходимости суду при отправлении правосудия учитывать постановления Пленума Верховного Суда РФ, принятые на основании статьи 126 Конституции РФ и содержащие разъяснения вопросов, возникших в судебной практике при применении норм материального или процессуального права, подлежащих применению в конкретном деле[65].

---

[64] Собрание законодательства РФ, 2016, — № 2 (ч. I). — Ст. 408.

[65] Бюллетень Верховного Суда РФ, 2004. — № 2. — С. 14.

В этом смысле представляет значительный практический интерес предложенная Г. Я. Стоякиным *классификация актов высших судебных органов*:

– *первая группа* актов включает в себя нормы — разъяснения, «не изменяющие и не дополняющие действующие нормы законодательных актов»;

– *вторая группа* представляют собой нормы — толкования, «причем толкование носит, как правило, распространительный характер»;

– *третья группа* состоит из *правовых норм*. По этой причине, каким бы новым термином ни называли устанавливаемые в постановлениях пленума Верховного Суда нормы общего характера, регулирующие общественные отношения, они по своей юридической силе и способу воздействия на участников этих отношений являются нормами права. И независимо от того, включены ли они впоследствии в состав другого нормативного акта или закреплены только в постановлении пленума, в случае их нарушения предусмотрена единая санкция процессуального характера — отмена или изменение решения суда[66].

Фактически в настоящее время *многие акты Верховного Суда РФ*, *во-первых*, *адресованы неопределенному кругу лиц*, *и*, *во-вторых*, *они имеют бóльшую силу*, *чем федеральные законы*. Следует также учитывать, что в части, не противоречащей актам Верховного Суда РФ, продолжают действовать акты Высшего Арбитражного Суда РФ.

Роль судебной практики особенно важна для сферы цифровых технологий в силу того, что они в настоящее время недостаточно урегулированы нормативными актами.

Кроме вышеуказанных документов, наиболее важные проблемы применения цифрового законодательства также рассмотрены в следующих судебных актах:

1. Обзор судебной практики Верховного Суда Российской Федерации, утв. Президиумом Верховного Суда РФ 4 июля 2018 г.

---

[66] Стоякин Г. Я. Роль судебной практики в формировании гражданского правоотношения // Актуальные проблемы гражданского права: межвуз. сб. науч. тр. — Свердловск, 1986. — С. 49–57. См. также: Подольская Н. А. К вопросу о понятии прецедента как источника права (общетеоретический аспект) // Судебная практика как источник права. — М.: Юристъ, 2000. — С. 152; Зайцев О. В. Роль судебных решений (прецедентов) и судебной практики в регулировании общественных отношений // Вестник гражданского процесса. — 2018. — № 2. — С. 105–136; и др.

2. Определение Верховного Суда РФ от 20 апреля 2018 г. № 78-КГ17-101.

3. Решение Суда по интеллектуальным правам от 7 сентября 2016 г. по делу № СИП-368/2016.

4. Апелляционное определение Санкт-Петербургского городского суда от 13 февраля 2017 г. № 33-2537/2017 по делу № 2-10119/2016.

5. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2018), утв. Президиумом Верховного Суда РФ 4 июля 2018 г.

6. Определение Верховного Суда РФ от 20 апреля 2018 г. № 78-КГ17-101.

7. Решение Суда по интеллектуальным правам от 7 сентября 2016 г. по делу № СИП-368/2016.

8. Апелляционное определение Санкт-Петербургского городского суда от 13 февраля 2017 г. № 33-2537/2017 по делу № 2-10119/2016.

Таким образом, *в настоящее время из всех судебных актов нормативный характер имеют только акты высших судебных органов*. Они содержат ряд принципиальных положений, которые пока еще не включены в законодательные акты.

Самое важное в главе 1

1. С учетом содержания принятых нормативных актов, необходимо *различать цифровизацию в узком и широком смыслах*. Под цифровизацией *в узком смысле* следует понимать меры по внедрению платформенных решений. Содержание понятия «цифровизация» *в широком смысле*, с учетом содержания нормативных актов, является практически необъятной. По состоянию на 16 мая 2021 г. в подзаконных актах содержится 32 значения данного понятия (например, обслуживание средств печати и копирования данных, услуги по предоставлению доступа в Интернет, местной и междугородней связи и т. д.). Термином «цифровизация» также обозначают понятия, которые раньше обозначали терминами «информатизация», «софтверизация» и «компьютеризация».

2. Меры защиты от угроз безопасности как физическим, так и юридическим лицам содержатся практически во всех отраслях законодательства, а не только законодательства о безопасности.

Предметом законодательства о безопасности являются действия публично-правовых субъектов по устранению угроз только неопределенному кругу лиц международными или государственными органами. В ином случае применяются *меры защиты*, закрепленные нормами иных отраслей законодательства.

3. В настоящее время *словосочетание* «*цифровая безопасность*» *используется только в подзаконных актах*. В последнем докладе Роспотребнадзора использован термин «кибербезопасность».

4. Роль судебной практики особенно важна для сферы цифровых технологий в силу того, что они в настоящее время недостаточно урегулированы нормативными актами.

Вопросы

1. Что понимается под цифровизацией в юридическом смысле?

2. Почему высока роль рецепции иностранного законодательства в сфере цифровизации?

3. Как содержание понятия «цифровизация» соотносится с содержанием понятий «информатизация», «софтверизация» и «компьютеризация»?

4. Какие общественные отношения являются предметом права экономической безопасности?

Список диссертаций

1. Аксенов И. А. Конституционно-правовые аспекты экономической безопасности Российской Федерации и роль органов внутренних дел в ее обеспечении. Дис. … канд. юрид. наук. — М., 2000.

2. Белов О. С. Органы внутренних дел в системе обеспечения экономической безопасности: организационные и правовые вопросы (по материалам Приволжского Федерального округа). Дис. … канд. юрид. наук. — М., 2004.

3. Блохин В. В. Правовое регулирование деятельности таможенных органов по обеспечению экономической безопасности Российской Федерации. Дис. … канд. юрид. наук. — М., 2004.

4. Герасимов А. П. Теоретико-правовые проблемы становления и развития экономической безопасности российской государственности (методологическое и историко-правовое исследование). Дис. ... д-ра юрид. наук. — СПб., 2001.

5. Генрих Н. В. Криминологические аспекты противодействия угрозам экономической безопасности России. Дис. … канд. юрид. наук. — М., 2002.

6. Горелов А. П. Уголовно-правовая охрана сферы предпринимательской деятельности как направление обеспечения экономической безопасности России. Дис. … канд. юрид. наук. — М., 2004.

7. Злобин В. В. Субъективное гражданское право и экономическая безопасность частных предпринимателей. Дис. … канд. юрид. наук. — М., 2003.

8. Игнатов Ю. В. Экономическая безопасность государств и проблемы ее международно-правового обеспечения в современных условиях. Дис. … канд. юрид. наук. — М., 2005.

9. Козырев А. А. Влияние института ответственности за налоговые правонарушения на экономическую безопасность государства. Дис. … канд. юрид. наук. — М., 2004.

10. Кочегин Д. В. Правовое регулирование деятельности органов государственной власти Читинской области в сфере обеспечения социально-экономической безопасности. Дис. ... канд. юрид. наук. — М., 2004.

11. Кочубей М. А. Криминологическое и уголовно-правовое обеспечение экономической безопасности Российской Федерации в сфере таможенной деятельности. Дис. … д-ра юрид. наук. — М., 2005.

12. Крючкова И. Н. Влияние экономических санкций Совета Безопасности Организации Объединенных Наций на исполнение частно-правовых договоров международного характера. Дис. … канд. юрид. наук. — М., 2005.

13. Курочкин В. Н. Правовое обеспечение инновационной деятельности в интересах экономической безопасности России. Дис. … канд. юрид. наук. — М., 2004.

14. Кутузов И. А. Нормативные основы гражданско-правового обеспечения экономической безопасности Российской Федерации. Дис. ... канд. юрид. наук. — М., 2006.

15. Ленковская Р. Р. Деятельность прокуратуры в системе обеспечения экономической безопасности Российской Федерации. Дис. ... канд. юрид. наук. — М., 2005.

16. Лысенкова Е. Н. Государственное правовое регулирование малого предпринимательства в целях обеспечения экономической безопасности Российской Федерации. Дис. ... канд. юрид. наук. — М., 2006.

17. Майорова Е. Н. Конституционные основы экономической безопасности в Российской Федерации. Дис. … канд. юрид. наук. — Челябинск, 2004.

18. Мусов Р. Х. Налоговые органы в системе обеспечения экономической безопасности. (Организационно-правовые аспекты). Дис. … канд. юрид. наук. — М., 2001.

19. Простова В. М. Экономическая безопасность России и проблемы прокурорского надзора. Дис. … канд. юрид. наук. — М., 1998.

20. Сенин В. И. Основы организации и функционирования Корпуса финансовой гвардии и Корпуса карабинеров в обеспечении экономической безопасности Италии. Дис. … канд. юрид. наук. — М., 2001.

21. Стрельников К. А. Правовые аспекты обеспечения экономической безопасности современного российского государства. Дис. … канд. юрид. наук. — Н. Новгород, 2004.

22. Сюсюкин А. В. Административно-правовое регулирование в сфере обеспечения экономической безопасности. Дис. … канд. юрид. наук. — Ростов н/Д, 2004.

23. Тимофеев С. В. Криминологические аспекты обеспечения экономической безопасности Российской Федерации. Дис. … канд. юрид. наук. — М., 2002.

24. Тропин С. А. Государственное управление в правоохранительной сфере в механизме обеспечения экономической безопасности России. Дис. … д-ра юрид. наук. — Рязань, 2004.

25. Хаупшев А. Х. Правовое обеспечение экономической безопасности и проблемы борьбы с организованной преступностью. (Региональный аспект). Дис. … канд. юрид. наук. — М., 1998.

26. Хрулев Д. А. Деятельность органов прокуратуры по обеспечению экономической безопасности России (организационно-правовые аспекты). Дис. … канд. юрид. наук. — М., 2005.

27. Чапчиков С. Ю. Теоретико-правовые аспекты защиты экономической безопасности Российской Федерации как функции государства. Дис. ... канд. юрид. наук. — М., 2006.

Список статей

1. Андреев В. К. О понятии цифровых прав и их оборотоспособности // Журнал предпринимательского и корпоративного права. — 2018. — № 2. — С. 38–41.

2. Василевская Л. Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. — 2019. — № 5. — С. 111–119.

3. Лаптева А. М. Правовой режим токенов // Гражданское право. — 2019. — № 2. — С. 29–32.

4. Новоселова Л. А. «Токенизация» объектов гражданского права // Хозяйство и право. — 2017. — № 12. — С. 29–44.

5. Белых В. С., Егорова М. А. Понятие, значение и правовое регулирование криптовалюты в современных условиях гармонизации и развитии цифровых правоотношений // Проблемы гармонизации экономических отношений и права в цифровой экономике / отв. ред. В. А. Вайпан, М. А. Егорова. — М.: Изд-во «Юстицинформ», 2020. — С. 221–229; Белых В. С., Болобонова М. О. Проблемы определения правового режима криптовалют // Журнал предпринимательского и корпоративного права. — 2019. — № 3. — С. 23–28.

6. Егорова М. А., Ефимова Л. Г. Понятие и особенности правового регулирования криптовалют // Предпринимательское право. — 2019. — № 3. — С. 11–16; Егорова М. А. К вопросу о понятии криптовалюты в европейском законодательстве: опыт для России // Право и цифровая экономика. — 2019. — № 3. — С. 11–13 и др.

7. Ефимова Л. Г. Криптовалюты как объект гражданского права // Хозяйство и право. — 2019. — № 4. — С. 17–25; она же. Некоторые аспекты правовой природы криптовалют // Юрист. — 2019. —№ 3. — С. 12–19.

8. Максуров А. А. К вопросу о юридической ответственности за использование криптовалюты при производстве расчетов // Вестник Омской юридической академии. — 2018. — № 4. — С. 428–433; он же. Криптовалюта как экономико-правовая категория // Современное право. — 2018. — № 9. — С. 68–71; он же. Криптовалюта в гражданском, семейном и трудовом праве России // Имущественные отношения в Российской Федерации. — 2018. — № 8. — С. 96–101.

9. Новоселова Л. А. О правовой природе биткойна // Хозяйство и право. — 2017. — № 9. — С. 21–29.

10. Савельев А. И. Криптовалюты в системе объектов гражданских прав // Закон. — 2017. — № 8. — С. 12–19; он же. Комментарий на положения о регулировании операций с криптовалютами и иных отношений, основанных на технологии блокчейна Декрета Президента Республики Беларусь «О развитии цифровой экономики» № 8 от 21 декабря 2017 г. // www.ssrn.com/abstract=3102872 и др.

11. Сидоренко Э. Л. Криптовалюта как новый юридический феномен // Общество и право. — 2016. — № 3. — С. 15–22.

12. Мажорина М. В. Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // Lex russica. — 2019. — № 2. — С. 107–120.

13. Максуров А. А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование. — М.: Корпорация «Дашков и К°», 2020.

14. Савельев А. И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. — 2017. — № 5. — С. 94–117; он же. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений // Закон. — 2018. — № 2. — С. 36–51.

15. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // ИПБ КонсультантПлюс.

16. Федоров Д. В. Токены, криптовалюта и смарт-контракты в отечественных законопроектах с позиции иностранного опыта // Вестник гражданского права. — 2018. — № 2. — С. 30–74.

17. Мохат П. М. Искусственный интеллект: правовой взгляд. — М.: Буки Веди, 2017.

18. Нестеров А. В. Возможны ли правоотношения и юридические взаимодействия между людьми и роботами? // Юридический мир. — 2017. — № 9. — С. 52–55.

19. Попова Н. Ф. Основные направления развития правового регулирования использования искусственного интеллекта, роботов и объектов робототехники в сфере гражданских правоотношений // Современное право. — 2019. — № 10. — С. 69–73.

Литература

1. Артемова С. Т., Жильцов Н. А., Чердаков О. И. Цифровой разрыв и конституционные гарантии цифрового равенства // Конституционное и муниципальное право. — 2020. — № 10. — С. 41–45.

2. Андрюхин Н. Г. Предпосылки, содержание и значение новых разъяснений Пленума Верховного Суда Российской Федерации о квалификации и доказывании преступлений экстремистской направленности, совершаемых с использованием сети Интернет // Вестник Московского университета МВД России. — 2019. — № 4. — С. 67–72.

3. Алиев В. М., Соловых Н. Н. Цифровая экономика поставила нас перед необходимостью решения проблемы обеспечения цифрового суверенитета // Безопасность бизнеса. — 2018. — № 3. — С. 18–22.

4. Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. — М.: Изд-во «Юриспруденция», 2013. — 552 с.

5. Гаврин Д. А. Методы правового регулирования в условиях цифровизации // Предпринимательское право. Приложение «Право и Бизнес». — 2019. — № 3. — С. 14–16.

6. Галузин А. Ф. Кибербезопасность как самостоятельный вид безопасности в странах АТР // Право и политика. — 2018. — № 2. — С. 275–284.

7. Головизнин А. В. К вопросу о соотношении понятий «система права» и «система законодательства» // Вестник Московского университета МВД России. — 2010. — № 12. — С. 81–84.

8. Ефремов А. А. Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве // Информационное право. — 2016. — № 4. — С. 25–28.

9. Кожевина О. В. Национальные правовые режимы России и Франции в сфере цифровой безопасности: компаративный анализ // Право и цифровая экономика. — 2020. — № 2. — С. 12–16.

10. Лебедь (Ефремова) В. В., Телешина Н. Н. Актуальные проблемы киберправа // Право. Журнал Высшей школы экономики. — 2014. — № 2. — С. 173–183.

11. Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. — 2017. — № 1. — С. 17–21.

12. Скиннер К. Человек цифровой: четвертая революция в истории человечества, которая затронет каждого. — М.: Манн, Иванов и Фербер, 2019.

Глава 2. Правовое регулирование интернет-отношений

2.1. Понятие и общая характеристика информации как объекта правового регулирования

Существует мнение, что современный уровень развития научного знания не позволяет дать точного и законченного определения такого основополагающего понятия как информация[67]. По этой причине действующее законодательство в области гражданского права не раскрывает содержание самой информации, которая участвует в гражданском обороте, как самостоятельный объект права, не дает определение понятия информации как объекта гражданского права и не раскрывает место информации в системе объектов гражданского права, что, в свою очередь, приводит к отсутствию реальной возможности воспользоваться своими правами на ту или иную информацию, а также защитой нарушенных прав в области информации, в связи с неурегулированностью данного вопроса в действующем законодательстве[68]. Однако в настоящее время действует огромное количество нормативных актов, регулирующих информационные отношения. Для определения предмета их регулирования необходимо определить юридические признаки информации.

Согласно общепринятой точке зрения, под *информацией* (от *лат*. informatio — разъяснение, изложение) понимаются сведения, то есть познания в какой-либо области, известия, сообщения, знания, представление о чем-либо, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом (например, с помощью условных сигналов, с использованием технических средств и т. д.), а также сам процесс передачи или получения этих сведений.

Нормативное определение информации является более кратким — это *сведения* (*сообщения*, *данные*) *независимо от формы*

---

[67] Информационные правоотношения: теоретические аспекты. — М.: Проспект, 2017. — С. 21. Автор главы — С. Г. Чубукова.

[68] Насонова Е. Н. Информация как объект гражданского права. Автореф. дис. ... канд. юрид. наук. — М., 2002. — С. 34.

их представления (п. 1 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»).

Как указывает П. У. Кузнецов, *информация как объект права* — правовая модель, обобщенный правовой образ конкретных нематериальных благ информационной природы (рекламы, персональных данных, статистической информации, геномной информации, кредитной истории, информационной продукции, электронного документа, электронной подписи и др.)[69].

В литературе принято выделять следующие *разновидности информации*:

– информация, создаваемая в процессе творчества (произведения науки и культуры, открытые патенты и авторские свидетельства);

– обязательно представляемая документированная информация;

– официальные документы;

– массовая информация, распространяемая СМИ;

– другая информация неограниченного доступа, информация ограниченного доступа;

– документированная информация, содержащая сведения о коммерческой тайне, ноу-хау (в порядке защиты секретов производства и науки);

– персональные данные (в порядке защиты личной тайны)[70].

К *основным признакам информации* принято относить:

1) непотребляемость;

2) возможность бесконечного тиражирования;

3) сохранение передаваемой информации у передающего субъекта;

4) подверженность не физическому, а моральному старению.

2.2. Сведения конфиденциального характера

Законодатель ввел термин «конфиденциальная информация», которым обозначают *любые сведения, доступ к которым запрещен или ограничен*. Они содержатся в Указе Президента РФ

[69] Кузнецов П. У. Информация как объект правоотношений в сфере обеспечения информационной безопасности // Труды Института государства и права РАН. — 2016. — № 3. — С. 46–47.

[70] Насонова Е. Н. Информация как объект гражданского права. Автореф. дис. ... канд. юрид. наук. — М., 2002. — С. 53.

от 6 марта 1997 г. (ред. от 13 июля 2015 г.) «Об утверждении Перечня сведений конфиденциального характера»:

1. Персональные данные, то есть сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц.

3. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц.

4. Сведения, связанные с профессиональной деятельностью, доступ к которым нормативно ограничен (профессиональные тайны — врачебная, адвокатская и т. д. тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений).

5. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

6. Служебная тайна.

7. Коммерческая тайна.

Таким образом, *в данном нормативном акте содержатся несистематизированный перечень и общая характеристика сведений конфиденциального характера*. *Регулирование отношений по поводу этих сведений производится нормами*, *содержащимися в других нормативных актах*.

2.3. Персональные данные

Интенсификация инновационного развития, обусловленная четвертой промышленной революцией, имея очевидных достоинств, потенциально является источником угроз, в том числе, и *в сфере персональных данных*. Как указал президент Всемирного экономического форума в Давосе К. Шваб, «четвертая промышленная революция изменит не только то, что мы делаем, но и то, кем мы являемся. На нас, индивидуумов, это окажет многоплановое влияние, скажется на нашей идентичности и различных гранях ее проявления: на наши представления

о неприкосновенности частной жизни». Законодатель, осознавая серьезность данной тенденции, был вынужден разработать систему нормативных актов, обеспечивающих минимизацию этих угроз. Базовое положение, содержащееся в статье 23 Конституции РФ, конкретизировано в законах и подзаконных актах.

Очевидно, что угроза личной жизни гражданина существовала всегда, но с появлением *автоматизированной обработки данных об индивидах* она резко усилилась. Согласно обоснованному мнению одного из диссертантов, с появлением автоматизированной обработки персональных данных и их размещением в открытых информационных сетях ситуация изменилась: возникла возможность несанкционированного использования баз данных, в том числе и в криминальных целях, то есть опасность нежелательного для гражданина разглашения конфиденциальной информации.

Именно для минимизации этих угроз была разработано понятие «персональные данные». Под ним понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (статья 3 федерального закона «О персональных данных»).

В тоже время цифровизация в ряде случаев обеспечивает больше гарантий правообладателям. Так, например, *цифровые данные в большей мере защищают конфиденциальную информацию*. В частности, как отмечают в литературе, «аналоговые удостоверения» — например, водительское удостоверение или паспорт — статичны и монолитны, поэтому невозможно предъявить лишь одну их часть или графу, а цифровые данные такую возможность предоставляют.

Проект закона «Об основном документе, удостоверяющем личность гражданина Российской Федерации» подготовлен с учетом данного обстоятельства.

Интенсификация инновационного развития, обусловленная четвертой промышленной революцией, кроме очевидных достоинств, потенциально является источником угроз, в том числе и в сфере персональных данных. Как указал президент Всемирного экономического форума в Давосе К. Шваб, «четвертая промышленная революция изменит не только то, что мы делаем, но и то, кем мы являемся. На нас, на индивидуумов,

это окажет многоплановое влияние, скажется на нашей идентичности и различных гранях ее проявления: на наши представления о неприкосновенности частной жизни»[71].

Серьезной проблемой, как отмечено в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, является необходимость соблюдения баланса между своевременным внедрением современных технологий обработки данных с защитой прав граждан, включая право на личную и семейную тайну.

В тоже время цифровизация в ряде случаев обеспечивает больше гарантии правообладателям. Так, например, *цифровые данные в большей мере защищают конфиденциальную информацию*. Так, в частности, «аналоговые удостоверения» — например, водительское удостоверение или паспорт — статичны и монолитны. Поэтому невозможно предъявить лишь одну их часть или графу. А цифровые данные такую возможность предоставляют[72].

В силу вышеизложенных аргументов подготовлен проект ФЗ «Об основном документе, удостоверяющем личность гражданина Российской Федерации». Согласно данному документу, основным документом, удостоверяющим личность гражданина Российской Федерации будет являться электронная идентификационная карта, содержащая визуальные и электронные носители информации с записанными на них персональными данными владельца, включая биометрические персональные данные. Как указано в пояснительной записке к законопроекту, необходимость введения электронной карты обусловлена, прежде всего, повышением защищенности документов граждан Российской Федерации, позволяющего снизить риски мошеннических действий по ее использованию.

Итак, одним из негативных последствий интенсификации инновационного развития страны и, соответственно, расширения использования искусственного интеллекта, облачных технологий, технологий больших данных, Интернета вещей и других информационных технологий, является *усиление угрозы*

---

[71] Шваб К. Четвертая промышленная революция. — М.: Изд-во Эксмо, 2017. — С. 119.

[72] Винья П., Кейси М. Машина правды. Блокчейн и будущее человечества. — М.: Изд-во «Манн, Иванов и Фербер», 2018. — С. 236.

доступа к информации о личной жизни граждан и ее неправомерного использования. Законодатель, осознавая серьезность данной тенденции, был вынужден разработать систему нормативных актов, обеспечивающих минимизацию этих угроз.

Основой отечественного законодательства в сфере персональных данных являются международные договоры, важнейшим из которых является Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.

Базовое положение, содержащееся в статье 23 Конституции РФ, конкретизировано системой нормативных актов, важнейшими из которых, очевидно, являются ФЗ «О персональных данных», Трудовой кодекс РФ и ряд других законов. Содержание этих документов нашло отражение в подзаконных актах, в частности, в Правилах обработки персональных данных в Министерстве науки и высшего образования России, утвержденные приказом Минобрнауки России от 26 июля 2018 г.

Предельно общая характеристика, содержащаяся в базовом документе о персональных данных, заставила законодателя конкретизировать вышеуказанное нормативное положение в других документах. Так, например, согласно пункту 3 статьи 42 федерального закона «О государственной гражданской службе Российской Федерации», запрещается обрабатывать и приобщать к личному делу гражданского служащего персональные данные о *членстве в профессиональных союзах*.

Всего же в настоящее время действует 131 федеральный закон, содержащий в том или ином объеме нормы о персональных данных. В ряде нормативных актов обнаруживаются существенные пробелы. Так, например, в федеральном законе «Об образовании в Российской Федерации» содержатся только две нормы о персональных данных — подпункта 10 пункта 1 статьи 6 и пункта 1 статьи 98. Данное обстоятельство может являться потенциальной причиной конфликтов субъектов образовательных отношений. Так, например, нет общепринятой точки зрения по поводу возможности предоставления информации об оценках, полученных студентом родителям и иным законным представителям. В локальных актах вузов, как правило, ограничиваются указанием на то, что, во-первых, все персональные данные студента следует получать у него самого

и, во-вторых, вуз может предоставить без письменного согласия студента передавать обрабатываемые персональные данные третьим лицам только в случаях, предусмотренных законодательством Российской Федерации.

Логический анализ действующего законодательства позволяет прийти к выводу о том, что информация об оценках, полученных студентом, может передаваться родителям и иным законным представителям без согласия студента в двух случаях: (1) если студент является несовершеннолетним и (2) если стороной договора оказания образовательной услуги являются родители или иные законные представители, а не сам обучающийся.

Действующее законодательство предоставляет, по общему положению, самому правообладателю возможность признавать ту или иную информацию конфиденциальной. Рядом нормативных актов установлены исключения из данной общей нормы. В частности, в статье 5 ФЗ «О коммерческой тайне» содержится перечень сведений, в отношении которых не может быть установлен режим коммерческой информации.

Очевидно, что угроза личной жизни гражданина существовала всегда, но с появлением *автоматизированной обработки данных об индивидах* она резко усилилась. Согласно обоснованному мнению одного из диссертантов, с появлением автоматизированной обработки персональных данных и их размещением в открытых информационных сетях ситуация изменилась: возникла возможность несанкционированного использования баз данных, в том числе и в криминальных целях, то есть опасность нежелательного для гражданина разглашения конфиденциальной информации[73].

Следует признать, что между определениями персональных данных, содержащихся в разных нормативных актах, нет «китайской стены». Более того, в ряде случаев их содержание может полностью совпадать. А в ФЗ «О системе государственной службы Российской Федерации» даже использован юридический прием двойной квалификации — согласно пункту 5 статьи 14 данного документа, в случаях, установленных федеральными законами и иными нормативными правовыми

[73] Белгородцева Н. Г. Теоретико-правовые аспекты защиты персональных данных: дис. ... канд. юрид. наук. — М., 2012. — С. 98.

актами Российской Федерации, персональные данные государственных служащих *могут быть* отнесены к сведениям, составляющим государственную тайну.

Определение понятия «персональные данные» в нормативных актах, излагается, как правило, с учетом специфики предмета их регулирования. В частности, применительно к муниципальным служащим, таковой является информация, необходимая представителю нанимателя в связи с исполнением муниципальным служащим обязанностей по замещаемой должности муниципальной службы и касающаяся конкретного муниципального служащего (ст. 29 ФЗ «О муниципальной службе в Российской Федерации»). Но эти отличия, как правило, не являются принципиальными.

Однако более разумным все-таки представляется включение в нормативный акт отсылочной нормы к базовому акту. Так, например, согласно пункту 1.1 статьи 5 ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», термины «персональные данные» и «оператор», используемые в данном нормативном акте, применяются в том значении, в каком они используются в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных». В силу мобильности системы правовых регуляторов, следует признать ошибочным ссылку на конкретный нормативный акт. Поэтому более предпочтительной является более абстрактная формулировка статьи 85.1 «Персональные данные пассажиров воздушных судов» Воздушного кодекса РФ: в целях ведения реестров лиц, воздушная перевозка которых ограничена, перевозчики осуществляют обработку персональных данных пассажиров в соответствии с законодательством Российской Федерации в области персональных данных.

Следует учитывать, что к тому моменту, когда отечественных законодатель, осознал необходимость создания особого правового режима для персональных данных, *уже существовала развернутая система норм, обеспечивающих защиту других разновидностей информации ограниченного доступа*. Иногда их смешивают. Это неправильно. Так, например, П. У. Кузнецов справедливо отмечает, что «В отличие от тайны, конфиденциальность данных не носит абсолютного

характера, поскольку при согласии субъекта сведения, не их составляющие, могут распространяться и передаваться третьим лицам. Более того, в Законе названы условия, при которых персональные данные могут распространяться и без согласия граждан»[74].

Соответственно, возникают проблемы соотношения регламентирующего воздействия правовых регуляторов *разновидностей информации ограниченного доступа*.

Пожалуй, наиболее обоснованной по данной проблеме является мнение М. В. Бундина, который считает, что в целях устранения возникающих коллизий, связанных с соотнесением правового режима конфиденциальности персональных данных с иными правовыми режимами конфиденциальной информации, такими как врачебная тайна, тайна связи, адвокатская, нотариальная, банковская тайны, обосновывается необходимость закрепления в Федеральном законе «О персональных данных» коллизионной нормы-правила, которая бы установила приоритет требований режима конфиденциальности персональных данных, которые должны быть выполнены конфидентами, в условиях, когда иными режимными требованиями предусматривается более низкий уровень защищенности информации[75].

Таким образом, цифровизация общественных отношений является новым вызовом, но и одновременно новым фактором повышения эффективности системы правовых актов в сфере защиты персональных данных.

2.4. Понятие и признаки сети Интернет

Под Интернетом в самом общем виде принято понимать всемирную систему объединенных компьютерных сетей для хранения и передачи информации. В российском законодательстве нет определения Интернета, но Россия является участником ряда международных договоров, принятых в рамках Содружества Независимых Государств (далее — СНГ). А в статье 2 Модельного Закона СНГ об основах регулирования Интернета 2005 г.,

---

[74] Кузнецов П. У. Информационное право. — М.: Изд-во «Юстиция», 2019. — С. 336.

[75] Бундин М. В. Персональные данные в системе информации ограниченного доступа. Автореф. дис. … канд. юрид. наук. — М., 2017. — С. 10.

Интернет определяется как глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц[76].

В национальных (внутригосударственных) нормативных актах содержатся, как правило, более краткие определения. Так, например, согласно украинскому законодательству, «Интернет — всемирная информационная система общего доступа, которая логически связана глобальным адресным пространством и базируется на Интернет-протоколе, определенном международными стандартами»[77].

В литературе отмечается, что в настоящее время при написании слова «Интернет» часто используется прописная буква, а не строчная (заглавная) буква, что знаменует переход этого понятия из категории имен собственных, как обозначения названия многоуровневой компьютерной сети, в категорию имен нарицательных, как обозначения коммуникационной инфраструктуры, обеспечивающей определенную технологию обмена информацией[78]. Однако, приказом Минобрнауки России от 8 июня 2009 г. № 195 был утвержден обновленный список словарей и справочников, содержащих нормы современного русского литературного языка при его использовании в качестве государственного языка Российской Федерации. И, соответственно, *слово* «*Интернет*» *нужно писать с большой буквы*. Очевидно, что это правило касается и Рунета — совокупности русскоязычных сайтов.

---

[76] Модельный Закон об основах регулирования Интернета, принят на 36-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление № 36-9 от 16 мая 2011 года) // http://zakon2.rada.gov.ua/laws/show/997_o14

[77] Закон Украины о телекоммуникациях от 18 ноября 2003 г. (ред. от 23 февраля 2014 г.). Статья 1 // http://kodeksy.com.ua/ka/o_telekomunikatsiyah/statja-1.htm

[78] Касенова М. Б. Правовое регулирование трансграничного функционирования и использования интернета. Дис. … д-ра юрид. наук. — М., 2016. — С. 50.

О соотношение понятий «Интернет», «киберпространство» и «информационно-телекоммуникационная сеть». Наряду с термином «Интернет» часто используются слова-архаизмы с приставкой «кибер-» («киберпреступность»[79], «киберправо» и т. д.). Они являются синонимами.

Сеть Интернет является разновидностью *информационно-телекоммуникационной сети*, под которой, согласно статье 2 федерального закона от 27 февраля 2006 г. (ред. от 29 июня 2018 г.) «Об информации, информационных технологиях и о защите информации», понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. А сам термин «телекоммуникация» происходит от *греч*. «tele» («вдаль») и *лат*. «communico» («делаю общим»), *лат*. «communication» — (сообщение, передача), т. е. речь идет о сообщениях/данных, которые передаются на расстояние и/или об информации, доступ к которой можно получить на расстоянии (информация становится «общей»). Этот термин в большей степени, чем термин «электросвязь», отражает суть оказываемых услуг по передаче сообщений / данных на расстояние и не зависит от используемых технологий (световые лучи, радиоволны, непосредственно электрические импульсы). Но в российском законодательстве в настоящее время вместо терминов «телекоммуникации», «телекоммуникационная компания» и «телекоммуникационные услуги» чаще используются термины «электросвязь», «организация электросвязи» и «услуги связи/электросвязи»[80].

Принято считать, что идея построения информационной сети была предложена Дж. Ликлайдером 1962 г. в серии статей о концепции построения «галактической сети» («Galactic Network»). Данная идея была реализована министерством обороны США

---

[79] Следует учитывать, что в англоязычной литературе приставка «cyber-» используется довольно часто для обозначения всей совокупности информационно-коммуникативных технологий и всех связанных с ними социальных явлений // Чекунов И. Г. Понятие и типология киберпреступности // Вестник Академии права и управления. — 2012. — № 26. — С. 69.

[80] Кузнецова О. А. Гражданско-правовое регулирование договорных отношений в сфере телекоммуникационных услуг: монография. — М.: Изд-во «Юстицинформ», 2018.

в 1967 г., когда был представлен план построения пакетной сети ARPANET. В 1969 четыре компьютера были соединены в первоначальную конфигурацию ARPANET — своего рода зародыш Интернета. В последующие годы число узлов ARPANET быстро росло путем подключения компьютеров различных государственных учреждений США. Ключевым событием в истории развития Интернета стало изобретение Р. Каном сетевого протокола, на базе которого в 1973 г. разработано семейство протоколов TCP/IP.

Следует учитывать, что *Интернет не является ни субъектом права и ни объектом права*. Правовые отношения порождает не Интернет как компьютерная сеть, а субъекты по поводу объектов, которые тем или иным образом связаны с такой сетью. Интернет как компьютерная сеть не создает каких-либо новых объектов и товаров, а лишь предоставляет возможности для их создания, размещения и реализации между пользователями сети[81].

К основным *юридическим признакам сети Интернет* относятся:

1. Субъектом электронных гражданских правоотношений может быть любой субъект гражданского права, имеющий доступ в Интернет.

2. Особенностями субъектов электронных гражданских правоотношений являются, во-первых, трудность определения дееспособности лица, с которым одна из сторон вступает в правоотношение, во-вторых, появление виртуальных организаций, которые создаются пользователями Интернет с целью осуществления коммерческой деятельности, в-третьих, использование так называемых программ-роботов, позволяющих вступать в правоотношения автоматически, в-четвертых, трудность в определении физического местонахождения других участников конкретного правоотношения.

3. Сеть Интернет не имеет собственника.

4. Совокупность формирующих ее сетей имеет различную географическую направленность, что не позволяет применять ко всей сети Интернет законодательство только одной страны.

---

[81] Глушков А. В. Проблемы правового регулирования интернет-отношений. Автореф. дис. … канд. юрид. наук. — СПб., 2007. — С. 12.

5. Сеть Интернет невозможно отключить целиком, так как ее маршрутизаторы, то есть сетевые компьютеры, которые связывают составляющие ее сети, не имеют единого внешнего управления.

6. Отношения в сфере Интернета регулируются нормами нескольких отраслей законодательства, наиболее важными из которых являются гражданское, административное и уголовное законодательства. Так, например, нормы права интеллектуальной собственности — подотрасли гражданского права устанавливают правовой режим доменных имен, регулируют хостинговые правоотношения, отношения между провайдерами и потребителями услуг и др. Санкции за интернет-правонарушения содержатся в административном и уголовном законодательствах[82].

Наиболее важные особенности интернет-отношений определены федеральным законом от 27 июля 2006 г. (ред. от 9 марта 2021 г.) «Об информации, информационных технологиях и о защите информации»[83]. Согласно данному нормативному акту, важнейшими элементами сети Интернет являются интернет-сайты и доменные имена. Интернет-сайты представляют собой информационные ресурсы, а доменные имена осуществляют адресацию в информационно-телекоммуникационной сети и индивидуализируют интернет-сайты. С помощью *интернет-сайтов*, которые являются по свое сути информационными ресурсами, информация распространяется за считанные минуты и безо всяких границ; а *доменные имена* обеспечивают адресацию запросов в информационно-телекоммуникационной сети Интернет и индивидуализируют интернет-сайты[84].

Важнейшими *субъектами интернет-отношений*, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», являются:

1) обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

---

[82] См. напр.: Быстров А. К. Интернет-сайт и доменное имя как объекты гражданских прав в системе отношений по использованию сети Интернет / дис. … канд. юрид. наук. — М., 2016. — С. 13; Глушков А. В. Ук. соч. — С. 12 и др.

[83] Собрание законодательства РФ, 2006. — № 31 (ч. 1). — Ст. 3448.

[84] Быстров А. К. Ук. соч. — С. 3–4.

2) оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

3) владелец сайта в сети «Интернет» (администратор сайта) — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте;

4) провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет». При этом под *хостингом* понимается способ размещения сайта в сети Интернет. Как только сайт будет размещен на сервере, пользователи Интернета получат к нему доступ, набрав в строке браузера доменное имя. А домен представляет собой имя сайта, его адрес в Интернете. Как правило, он выглядит так: http://www.site.ru Домен может располагаться в различных территориальных зонах. Для России это зоны ru и su.

Существуют *три основные модели нормативного регулирования общественных отношений в сети Интернет*:

1. *Авторитарная модель*, которая характеризуется установлением строгих законов или иных санкционируемых государством запретов, как правило, в рамках внутригосударственной компетенции и без учета норм международного права. Авторитарная модель характерна для государств Азиатско-Тихоокеанского региона, но в той или иной мере имеет распространение во всем мире. Данной модели правопонимания соответствует ограничение возможности доступа пользователей в сеть Интернет и установление цензуры.

2. *Либертарная модель*, получившая распространение в США в середине 90-х гг. XX в., основана на строгом соблюдении конституционных прав личности, гарантирующих отсутствие цензуры и свободу самовыражения. В последние годы несколько теряет популярность в связи с глобальными угрозами национальной безопасности, а также под давлением крупных правообладателей и их объединений, вызванным нарастающей угрозой их экономическому благополучию в сфере интеллектуальных прав.

3. *Технологическая модель* — естественная модель, в рамках которой наибольшее значение приобретает не законодательство (которое зачастую не может служить эффективным регулятором отношений в сфере использования сети Интернет), а научно-технические особенности и технические способы регулирования общественных отношений в сети Интернет. Особая роль в процессе регулирования отводится, как и в либертарной модели, общественному самоуправлению в сети Интернет, обычаям делового оборота и этическим нормам. Технологическая модель правопонимания отношений в сети Интернет характеризуется тем, что все участники правоотношений, в том числе и государство, исходят исключительно из многофункциональных реалий глобальных телекоммуникационных сетей[85].

2.5. Рунет

Надзор за российской частью Интернета — *Рунетом* — осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и другие профильные ведомства.

Основой регулирования взаимоотношений в Рунете являются следующие, утвержденные правительством РФ, документы:

1. Временный регламент исполнения государственной функции создания, формирования и ведения единой автоматизированной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено».

2. Порядок взаимодействия оператора реестра с провайдером хостинга, Рекомендации по организации и техническим решениям по ограничению операторами связи доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, которые

[85] Дашян М. С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. — М.: Изд-во «Волтерс Клувер», 2007. — С. 30.

размещены на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций[86].

1 ноября 2019 года вступил в силу федеральный закон от 1 мая 2019 года «О внесении изменений в Федеральный закон "О связи"». Его именуют также *законом о суверенном Рунете*. Этим документом предусмотрено создание *национальной системы маршрутизации интернет-трафика* и устанавливаются следующие правила:

1) вводится национальная система доменных имен;

2) реализуется возможность централизованного управления Рунетом;

3) оптимизируется, с учетом приобретенного опыта, механизм ограничение доступа к запрещенным интернет-ресурсам;

4) операторы обязаны установить отечественное оборудование на точках обмена трафиком внутри страны и линиях связи, пересекающих границу РФ;

5) обмен трафиком между операторами связи должен осуществляться только через точки обмена, внесенные в специальный реестр, порядок включения в который будет определен правительством РФ.

2.6. Договоры, заключаемые в сети Интернет

Договоры, заключаемые в сфере Интернета, принято разделять на четыре группы:

1) договоры, связанные с доступом к сети Интернет, местом заключения которых является реальное физическое пространство. Стандартным видом таких договоров является договор об оказании провайдерских услуг (договор доступа);

2) договоры, также связанные с доступом к сети, но совершаемые уже в виртуальном пространстве. К ним можно отнести договоры, связанные с доменными именами, договоры

[86] Постановление Правительства РФ от 26 октября 2012 г. № 1101 (ред. от 5 июня 2018 г.) «О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов", позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено»// ИПБ «Консультант-плюс».

функционирования базовых элементов технологической структуры Интернета — корневых серверов и других систем управления Интернетом и др.;

3) традиционные договоры, но уже имеющие электронную форму и заключаемые в виртуальном пространстве. Это наиболее многочисленная группа договоров, к которым относятся как договоры коммерческого характера, так и договоры об оказании информационных услуг при пользовании Интернетом;

4) договоры, заключаемые в Интернете, связанные с использованием объектов авторских и смежных (в том числе созданных в виртуальном пространстве) прав. Эти договоры связаны в основном с разработкой различных компьютерных программ. Примером такого договора можно назвать договор на выполнение работ по разработке сайта[87].

Самое важное в главе 2

1. Под Интернетом в самом общем виде принято понимать всемирную систему объединенных компьютерных сетей для хранения и передачи информации. Наряду с термином «Интернет» принято использовать слова-архаизмы с приставкой «кибер-» («киберпреступность», «киберправо» и т. д.). С юридической точки зрения они являются синонимами.

2. Интернет не является ни субъектом права и ни объектом права. Правовые отношения порождает не Интернет как компьютерная сеть, а субъекты по поводу объектов, которые тем или иным образом связаны с такой сетью.

3. К основным юридическим признакам сети Интернет относятся: (1) субъектом электронных гражданских правоотношений может быть любой субъект гражданского права, имеющий доступ в Интернет; (2) особенностями субъектов электронных гражданских правоотношений являются, во-первых, трудность в определении дееспособности лица с которым одна из сторон

[87] См. напр.: Типовые договоры об использовании объектов авторских и смежных прав / под ред. Г. И. Уваркина. — М., 2010. — С. 2; Абдуджалилов А. Правовая характеристика договоров, заключаемых в Интернете // Журнал российского права. — 2016. — № 2. — С. 77 и др.

вступает в правоотношение, во-вторых, появления виртуальных организаций, которые создаются пользователями Интернет с целью осуществления предпринимательской деятельности, в-третьих, использование так называемых программ-роботов, позволяющих вступать в правоотношения автоматически, в-четвертых, трудность в определении физического местонахождения других участников конкретного правоотношения; (3) сеть Интернет не имеет собственника; (4) совокупность формирующих ее сетей имеет различную географическую направленность, что не позволяет применять ко всей сети Интернет законодательство только одной страны; (5) сеть Интернет невозможно отключить целиком, так как ее маршрутизаторы, то есть сетевые компьютеры, которые связывают составляющие ее сети, не имеют единого внешнего управления и (6) отношения в сфере Интернета регулируются нормами нескольких отраслей законодательства.

4. Существуют три основные модели нормативного регулирования общественных отношений в сети Интернет: авторитарная, либертарная и технологическая.

5. Договоры, заключаемые в области Интернета, принято разделять на четыре группы: (1) договоры, связанные с доступом к сети Интернет, местом заключения которых является реальное физическое пространство; (2) договоры, также связанные с доступом к сети, но совершаемые уже в виртуальном пространстве; (3) традиционные договоры, но уже имеющие электронную форму и заключаемые в виртуальном пространстве и (4) договоры, заключаемые в Интернете, связанные с использованием объектов авторских и смежных прав.

Вопросы

1. Юридическое определение Интернета. Как соотносятся содержание понятий «Интернет», «киберпространство» и «информационно-телекоммуникационная сеть»?

2. Юридические признаки Интернета.

3. Правовой статус субъектов интернет-отношений.

4. Модели нормативного регулирования общественных отношений в сети интернет.

5. Договоры, заключаемые в сфере Интернет.

Нормативные акты

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Российская газета, 06.12.2016.

2. Постановление Правительства РФ от 15 апреля 2014 № 313 (ред. от 30 марта 2018 г.) «Об утверждении государственной программы Российской Федерации “Информационное общество (2011–2020 годы)”».

3. Федеральный закон от 27 июля 2006 г. (ред. от 9 марта 2021 г.) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 2006. — № 31 (ч. 1). — Ст. 3448.

4. Модельный закон об основах регулирования Интернета от 25 ноября 2016 г. // www.iacis.ru

5. Закон Свердловской области от 14 мая 2010 г. (ред. от 24 сентября 2018 г.) «О порядке утверждения перечней информации о деятельности государственных органов Свердловской области, размещаемой в информационно-телекоммуникационной сети “Интернет”» // Областная газета, 26.09.2018.

Литература

1. Абдуджалилов А. Правовая характеристика договоров, заключаемых в Интернете // Журнал российского права. — 2016. — № 2. — С. 71–82.

2. Алиев В. М., Соловых Н. Н. Цифровая экономика поставила нас перед необходимостью решения проблемы обеспечения цифрового суверенитета // Безопасность бизнеса. — 2018. — № 3. — С. 18–22.

3. Андрющенко Е. С. Интернет-отношения: государственное регулирование и самоуправление / дис. ... канд. юрид. наук. — Саратов, 2010.

4. Барановский П. Д. Международно-правовые проблемы охраны интеллектуальной собственности в сети Интернет: автореф. дис. ... канд. юрид. наук. — М., 2005.

5. Басманова Е. С. Интернет-сайт как объект имущественных прав: дис. … канд. юрид. наук. — М., 2010.

6. Бачило И. Л. Интернет как явление для системы права // Проблемы информатизации. — М., 2000. — № 3. — С. 3–12.

7. Головизнин А. В. Интернет как объект правового регулирования // Актуальные проблемы цивилистических отраслей права. Сборник научных трудов / под ред. А. В. Головизнина. — Екатеринбург: Изд-во УРЮИ МВД России, 2018. — С. 6–11.

8. Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: дис. ... канд. юрид. наук. — Екатеринбург, 2003.

9. Жарова А. К. Правовые проблемы обращения информации в Интернете. Опыт Республики Узбекистан: дис. ... канд. юрид. наук. — М., 2002.

10. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. — 2014. — № 5. — С. 140–145.

11. Зинина У. В. О проекте модельного закона СНГ «Об Интернете» // Информационное право. — 2008. — № 1. — С. 23–31.

12. Касенова М. Б. Интернет и международное публичное право: ретроспектива доктринальных подходов // Международное публичное и частное право. — 2012. — № 2. — С. 18–24.

13. Кондратьева Е. А. Интернет-сайт — «новый» объект авторских прав // Юрист. — 2014. — № 12. — С. 38–40.

14. Крупко С. И. Правовые проблемы разрешения трансграничных споров, связанные с нарушением исключительных прав // Хозяйство и право. — 2015. — № 1 (456). — С. 41–56.

15. Кузнецов П. У. Теоретические основания информационного права: дис. ... д-ра юрид. наук. — Екатеринбург, 2005.

16. Лопатин В. Н. Информационная безопасность России. Дис. ... д-ра юрид. наук. — СПб., 2000.

17. Мансуров Г. З. Коммерческая тайна как разновидность конфиденциальной информации // Проблемы современной науки и образования. — 2014. — № 4 (22). — С. 69–71.

18. Мансуров Г. З. Банковская тайна как разновидность конфиденциальной информации // Наука, техника и образование. — 2014. — № 2 (2). — С. 92–94.

19. Мальцев А. С. Коллизионно-правовое регулирование трансграничных гражданско-правовых отношений, возникающих в процессе электронного взаимодействия. Дис. … канд. юрид. наук. — М., 2006.

20. Минбалеев А. В. Основы правового регулирования сети Интернет // Право и кибербезопасность. — 2014. — № 1. — С. 20–26.

21. Право цифровой экономики: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — М.: Изд-во «Проспект», 2020.

22. Рассолов И. М. Право и Интернет: теоретические проблемы. Дис. … канд. юрид. наук. — М., 2008.

23. Савельев А. И. Гражданско-правовое регулирование договоров между клиентом и Интернет-провайдером в сети Интернет. Дис. … канд. юрид. наук. — М., 2008.

24. Пахомова Е. П. Правовая природа и нормативно-правовое регулирование интернет-услуг по законодательству Российской Федерации // Юридический мир. — 2016. — № 9. — С. 34–37.

25. Погуляев В. Об «интернет-праве» // ЭЖ-Юрист. — 2004. — № 34. — С. 20–21.

26. Пучков В. О. Информация — объект гражданского права? // Арбитражные споры. — 2020. — № 2. — С. 135–144.

27. Рустамбеков И. Р. Об определении правового понятия сети Интернет // Информационное право. — 2015. — № 3. — С. 22–26.

28. Серго А. Г. Правовой режим доменных имен и его развитие в гражданском праве: дис. … д-ра юрид. наук. — М., 2011.

29. Стрельцов А. А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. ... д-ра юрид. наук. — М., 2004.

30. Талимончик В. П. Международно-правовое регулирование отношений информационного обмена. — М.: Изд-во «Юридический центр Пресс», 2011.

Глава 3. Риски и угрозы цифровой трансформации. Общая характеристика правового воздействия на угрозы

3.1. «Риск» и «экономическая угроза» как экономико-правовые понятия

Риск является экономико-правовым понятием в том смысле, что одноименный термин вначале появился в экономическом обороте и потом, спустя значительный промежуток времени, получил закрепление в нормативных актах. В самом общем виде под риском (от *фр.* — risqué) принято понимать *возможность возникновения обстоятельств*, *причиняющих материальный ущерб*, *угроза потерь*[88].

Понятие «риск» является предметом постоянного внимания юристов, как в советский, так и постсоветские периоды развития цивилистики. Как указывал еще в 1925 году Я. М. Магазинер, «право есть не что иное, как система распределения рисков, которая изменяет и направляет стихийно складывающееся их распределение на основе естественных законов экономики»[89].

Функциональное назначение данной категории, согласно господствующей в юриспруденции точке зрения, сводится к следующему: «используя институт риска, государство (путем издания нормативных актов) и предприниматели (путем заключения соглашений) устанавливают правила, которые позволяют, с одной стороны, свести к минимуму возможные вредоносные последствия, и, с другой стороны, если все же таковые будут иметь место, распределить убытки между участниками экономического оборота (участниками сделки)»[90]. В целом, соглашаясь с данным утверждением, считаем необходимым обратить внимание на то, что риски несут в ряде случаев не только отрицательные, но и положительные последствия.

---

[88] Захаренко Е. Н., Комарова Л. Н., Нечаева И. В. Новый словарь иностранных слов. — 3-е изд. — М.: ООО «Азбуковник», 2008. — С. 735.

[89] Магазинер Я. М. Общая теория права на основе советского законодательства // Правоведение. — 1999. — № 1. — С. 136.

[90] Панарина М. М. Способы минимизации бизнес-рисков: правовая природа, виды и анализ рисков // Право и экономика. — 2016. — № 3. — С. 19.

В литературе принято обращать внимание на *различия риска в экономическом и юридическом понимании*. Так, по мнению Д. А. Горячкиной, «Экономическая сущность риска состоит в наступлении для стороны обязанности в виде принятия на себя убытков, порожденных рисковыми обстоятельствами. Юридическая сторона риска заключается не в сути и идентификации рисковых обстоятельств, а в возможности выбора правовых средств, которые бы позволили предвидеть существующую вероятность наступления негативных имущественных последствий, минимизировать их и соотнести с желаемым имущественным интересом»[91].

Д. Р. Канев уточняет вышеизложенную формулировку следующим образом: «Гражданское право не способно предотвратить отрицательные имущественные последствия случайных обстоятельств, но оно должно урегулировать отношения сторон на случай наступления таких последствий»[92].

По мнению специалистов, существуют следующие *угрозы цифровой трансформации*:

– Кибертерроризм и кибершпионаж, ведущиеся против России США, их союзниками, а также другими странами и иностранными террористическими и преступными организациями, а также отдельными лицами и группами лиц.

– Те же угрозы со стороны внутренних преступных сообществ, террористических организаций, радикальных религиозных, нацистских и прочих экстремистских группировок и антигосударственных сил.

– Уход от налогообложения, незаконный вывоз капитала, отмывание преступно полученных доходов с использованием криптовалют.

– Осуществление незаконной предпринимательской деятельности посредством использования сети Интернет, включая электронную торговлю и финансовые услуги[93].

---

[91] Горячкина Д. А. Управление рисками в российском гражданском праве / автореф. дис. ... канд. юрид. наук. — М., 2013. — С. 7–8.

[92] Канев Д. Р. Распределение риска случайных убытков в российском гражданском праве / автореф. ... канд. юрид. наук. — СПб., 2013. — С. 9.

[93] Цифровая цивилизация. Россия и «электронный» мир XXI века / А. А. Проханов и др. — М.: Изд-во «Изборский клуб», 2018. — С. 46. Автор главы — С. Ю. Глазьев.

Под угрозой экономической безопасности, согласно Стратегии экономической безопасности Российской Федерации на период до 2030 года, утвержденной Указом Президента Российской Федерации от 13 мая 2017 г. № 208, принято понимать совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам Российской Федерации в экономической сфере.

В литературе содержание данного понятия толкуется шире: под экономической безопасностью страны можно понимать обеспеченность требуемого уровня национальной безопасности собственными финансовыми и другими ресурсами, создание благоприятных условий для развития экономики и повышения уровня конкурентоспособности страны, защищенность жизненно важных интересов личности, общества и государства в экономической сфере от внутренних и внешних угроз[94].

Из обширного перечня угроз, включенных в Стратегию экономической безопасности Российской Федерации на период до 2030 года, к цифровой сфере относятся следующие:

1) стремление развитых государств использовать свои преимущества в уровне развития экономики, высоких технологий (в том числе информационных) в качестве инструмента глобальной конкуренции;

2) использование дискриминационных мер в отношении ключевых секторов экономики Российской Федерации, ограничение доступа к иностранным финансовым ресурсам и современным технологиям;

3) подверженность финансовой системы Российской Федерации глобальным рискам (в том числе в результате влияния спекулятивного иностранного капитала), а также уязвимость информационной инфраструктуры финансово-банковской системы;

4) слабая инновационная активность, отставание в области разработки и внедрения новых и перспективных технологий (в том числе технологий цифровой экономики), недостаточный уровень квалификации и ключевых компетенций отечественных специалистов.

---

[94] Ускова Т. В. Ключевые угрозы экономической безопасности России // Проблемы развития территории. — 2019. — № 1 (99). — С. 8.

3.2. Правовые аспекты минимизации угроз в социальных сетях

В литературе под *социальной сетью* в самом общем виде понимается идентифицируемая уникальным веб-адресом программная система, которая используется для общения субъектов, имеющих общий круг интересов.

Как известно, на важность социальных сетей для изучения социального общества одним из первых обратил внимание основатель социометрии Я. Л. Морено, по мнению которого, «Существуют более или менее прочные структуры, объединяющие индивидов и социальные атомы в больших сетях»[95]. Сам термин «социальная сеть» был введен в научный оборот Дж. Барнсом в работе «Классы и собрания в норвежском островном приходе» еще в 1954 году[96]. Одной из современных тенденций является стремительная виртуализация социальных связей. Существует даже мнение, что сформировалась новая, виртуальная реальность, влияние которой на процессы, происходящие в обществе, растут лавинообразно и касаются практически всех областей общественной жизни[97].

Важнейшими разновидностями виртуальной реальности являются как общие (Facebook, Badoo, Instagram, Livejournal, YouTube, Twitter, Instagram, Telegram, ВКонтакте и др.), так и специализированные (Linkedln, Xing, Last.fm, Pinterest, DeviantART, Закон.ru и др.) социальные сети.

В настоящее время повседневной реальностью стали *иностранные социальные сети*. Серьезной проблемой является то, что подавляющее большинство социальных сетей, используемых российскими гражданами, являются иностранными. Альтернативные отечественные сети имеются, например, «Одноклассники» и «Вконтакте», но они пользуются гораздо меньшим спросом. Принадлежность другому государству затрудняет контроль и создает трудности для привлечения их правообладателей

---

[95] Морено Я. Л. Социометрия: экспериментальный метод и наука об обществе. — М.: «Академический проект», 2001. — С. 15.

[96] Barnes J. A. Class and Committees in a Norwegian Island Parish // Human Relations. 1954. Vol. 7. № 1. P. 39–58 / Цит. по: http://pierremerckle.fr/wp-content/uploads/2012/03/Barnes.pdf

[97] Тягунова Л. А. Виртуализация социума: сущность и тенденции / автореф. дис. … канд. филос. наук. — Саратов, 2007. — С. 3.

к ответственности в случаях нарушения ими российского законодательства. Как отмечает один их специалистов, «Социальные сети на сегодняшний день являются самой перспективной площадкой для ведения информационных войн. Широкий спектр возможностей при низких затратах делают новые медиа особенно эффективными в контексте манипулирования информацией»[98]. Кроме того, как указывает Н. Касперская, надо учитывать, что сами технологии мессенджеров — это так называемые облачные сервисы. Это значит, что хранилища данных находятся где-то в «облаке». Эти «облака», находятся за пределами РФ. Это означает, что мы не можем контролировать, что с ней дальше там происходит[99].

Юрисдикционные органы определяют дефиницию «социальная сеть» как *интерактивный многопользовательский автоматизированный проект, позволяющий создавать персональные учетные записи, размещать информацию в соответствии с пользовательским соглашением информационно-телекоммуникационной платформы Интернет пространства, а также осуществлять возмездные сделки* (*в частности, развивать через группы и сообщества пользователей магазины*)[100].

В литературе в качестве важнейших принято указывать следующие *признаки социальный Интернет-сетей*:

1) широко распространенное общественное явление, направленное на построение социальных связей, формирование групп и сообществ на основе этических и правовых норм;

2) телекоммуникационная платформа для построения связей, которая позволяет рассматривать социальную интернет-сеть уже как средство не только коммуникации, но и массового распространения информации;

3) трансграничное виртуальное общение, обеспеченное пользователям социальных интернет-сетей[101].

---

[98] Бутусов А. В. Социальные сети как инструмент политического противоборства и информационных войн // Вестник Тамбовского университета. — 2018. — Т. 4. — № 13. — С. 72–73.

[99] Касперская Н. О цифровых угрозах // https://zavtra.ru/blogs/o_tcifrovih_ugrozah

[100] См. напр.: Решение Арбитражного суда г. Москва от 16 апреля 2012 г. по делу № А-40-90178/10 // СПС Консультант-плюс.

[101] Перчаткина С. А. и др. Социальные интернет-сети: правовые аспекты // Журнал российского права. — 2012. — № 5. — С. 15.

В настоящее время предметом специального регулирования являются общение в сетях с посещаемостью более 500 000 пользователей в сутки. Основным требованием к ним, установленным так называемым *законом о социальных сетях*, является обязанность самостоятельно выявлять и блокировать запрещенные контент (федеральный закон «Об информации, информационных технологиях и о защите информации», ст. 10.6).

Из анализа средств массовой информации следует, что *наиболее частыми нарушениями в социальных сетях* являются (1) использование двойных стандартов при оценке событий в России и в западных странах; (2) размещение информации, направленной на нарушение территориальной целостности России и (3) нарушения прав российских граждан.

Так, например, 6 января 2021 года толпа протестующих, поддерживающих попытки президента США Д. Трампа отменить результат президентских выборов 2020 года, совершила несанкционированный властями вход в Капитолий США. Twitter и Facebook заблокировали аккаунты Трампа и удалили сообщения, связанные с инцидентом. Штурм Капитолия ими был квалифицирован как попытка государственного переворота. И наоборот, антиправительственные высказывания Навального этими же сетями никак не блокировались. И даже наоборот находили полную поддержку. Как отмечается в литературе, «число комментариев, содержащих призывы к насилию и дискриминации в социальных сетях, ежегодно увеличивается на 30 %. Кроме «Facebook», чиновники из ООН называют аналогичными полями для агитации такие популярные сервисы, как «Twitter», «Google»[102].

Еще одним из примеров русофобской деятельности является размещение в видеохостинге Ютуб ролика IX Форума свободной России, состоявшегося 20 ноября 2020 г. в Вильнюсе. Участниками данного мероприятия были высказаны суждения о необходимости расчленения России. В частности, по их мнению, «в нынешних границах России быть не может», «На месте этого кровавого монстра (России) должно быть десять удельных княжеств, которые занимались бы внутренними разборками и воевали друг с другом» и т. д.

---

[102] Бураева Л. А. Социальные сети как угроза информационной безопасности // Пробелы в российском законодательстве. — 2017. — № 3. — С. 72.

Таким образом, *важнейшей задачей в сфере обеспечения цифровой безопасности государства в настоящее время является обеспечение эффективного контроля за иностранными социальными сетями*.

3.3. Общая характеристика правового воздействия на цифровые угрозы

Термин «цифровизация» появился сравнительно недавно и поэтому в нормативных и правоприменительных актах, устанавливающих санкции, он еще не используется. Анализ нормативных актов позволяет выявить отсутствие единого варианта толкования данного термина, а правонарушения в цифровой сфере традиционно именуются «компьютерными правонарушениями», «интернет-преступлениями», «информационными правонарушениями» и т. д. Очевидно, что необходимо унифицировать используемую терминологию. За основу представляется необходимым взять следующее утверждение: «Использование элемента «цифровой» в понятии «цифровые данные» позволяет сделать акцент на том, что сюда включаются только те данные, которые могут быть обработаны компьютером»[103].

В самом общем виде правонарушения в сфере цифровых отношений представляется возможным квалифицировать на (1) классические, которые прямо упомянуты в российских нормативных актах (например, хищение, мошенничество и т. д.) и (2) специальные нарушения, для наименования которых используются, как правило, термины, реципированные из иностранных нормативных актов (кардинг, спаминг, фишинг, DDoS-атаки и т. д.).

Соответственно уголовным законодательством закреплены следующие группы информационных преступлений:

1) *специфические информационные преступления* — те деяния, которые могут быть совершены только с использованием информационных технологий или информационно-телекоммуникационных сетей. В первую очередь это компьютерные преступления;

---

[103] Мефодьева К. А. Цифровые данные как объект гражданско-правового регулирования в Германии, США и России / дис. … канд. юрид. наук. — М., 2019. — С. 24.

2) *преступления общеуголовного характера*, в которых применение информационных технологий и информационно-телекоммуникационных сетей существенно облегчает совершение преступного деяния или сокрытие его следов, дает возможность систематического и массового совершения преступных деяний. Например, получение взятки электронными деньгами или криптовалютой. При таком способе совершения преступления исключается непосредственный контакт между взяткодателем и взяткополучателем, крайне затруднительным становится установление факта получения материальной выгоды взяткополучателем;

3) *преступления общеуголовного характера*, при совершении которых могут использоваться информационные технологии и информационно-телекоммуникационных сетей, но они значительного влияния на преступный результат не оказывают. Например, замышляя убийство группой лиц по предварительному сговору, соучастники могут обмениваться сообщениями по сети Интернет, однако существенной роли в механизме преступления это не играет[104].

Следует также учитывать, что многие цифровые правонарушения являются разновидностью правонарушений в сфере интеллектуальной собственности и в сфере личных неимущественных прав, не связанных с имущественными, например, распространение клеветнической информации.

Еще одной важной особенностью правонарушений является *незаконченность разработки системы нормативных актов в сфере цифровых отношений*. Данное обстоятельство создает большие трудности для квалификации правонарушений в сфере цифровых отношений. Так, например, неопределенность правовой природы криптовалют.

Для цифровых правонарушений характерна *транснациональность* (*трансграничность*). Как отмечается в литературе, интернет-преступления совершаются, как правило, на территории нескольких стран. При этом нет ясности, территорию какой страны следует признавать местом совершения преступления: место

[104] Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex russica. — 2018. — № 4. — С. 111.

расположения оборудования (сервера), место нахождения лиц, совершивших преступление, или место наступления последствий преступления[105].

Принято считать, что интернет-преступление считается *совершенным на территории РФ*, если начинается оно за границей или там осуществлялись организаторская деятельность, подстрекательство, пособничество, а оканчивается на территории РФ.

Интернет-преступление следует также считать *совершенным на территории РФ*, если приготовительная деятельность для последующего совершения преступления за границей осуществлялась в России, а последствия в виде материального ущерба наступили за рубежом. Для преступлений, выполненных соучастниками, находившимися в разных государствах, местом совершения преступления для каждого соучастника будет территория того государства, где он выполнял свое преступное действие, определяемое разновидностью соучастника. По этому вопросу интересной представляется следующее мнение: если организатор, подстрекатель, пособник, исполнитель находятся на территории разных государств, местом совершения преступления признается территория того государства, где соучастник осуществил свою преступную роль в совместном совершении преступления[106].

Трансграничность совершаемых преступлений обуславливает также необходимость учета *принципа двойной криминализации деяния*. Дело в том, что различие в криминализации деяния в стране, с территории которой действовал правонарушитель и в государстве, где находится потерпевший, может сделать невозможным привлечение к ответственности.

Так, например, квалификация фишинга по Уголовному кодексу РФ является наиболее сложной. На первый взгляд, руководствуясь пунктом 21 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике

---

[105] Гузеева О. С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опыт, анализ, практика. — 2013. — № 10. — С. 17.

[106] Гузеева О. С. Ук. соч. — С. 18; Комментарий к Уголовному кодексу РФ / отв. ред. А. И. Рарог. — М., 2018. — С. 20 и др.

по делам о мошенничестве, присвоении и растрате», фишинг можно квалифицировать как кражу, так как для него не важно, каким образом добыты персональные данные потерпевшего, при условии, что виновным не было оказано воздействие на программное обеспечение или компьютерные сети. Однако предметом кражи могут являться только предметы материального мира, к которым не относятся, например, криптовалюта. Определенные сложности также вызывает квалификация фишинга по статье 272 Уголовного кодекса РФ, поскольку постановление Пленума Верховного Суда РФ № 48 не относит изменение данных о состоянии счета и движении криптовалюты к воздействию на цифровое пространство. При этом получение персональных данных пользователей посредством фишинга, в соответствии со статьей 274 Уголовного кодекса РФ, нарушает правила хранения, обработки и передачи компьютерной информации, однако такие действия, в соответствии с пунктом 20 постановления Пленума Верховного Суда РФ № 48, должны признаваться *мошенничеством в сфере компьютерной информации* и квалифицироваться по статье 159.6 Уголовного кодекса РФ[107].

Большое количество иностранных нормативных актов среди источников правового регулирования обусловлено тем, что цифровые технологии в нашей стране являются в основном заимствованными. Частным случаем данного обстоятельства является «*импорт*» *способов совершения правонарушений* и, соответственно, *активное использование иностранной терминологии*. В тоже время следует отметить, что и в нашей стране компьютерные преступления фиксировались правоохранительными органами еще в советские времена. Так, в СССР первые компьютерные преступления были выявлены в 1979 году в Вильнюсе (ущерб государству составил 78 584 руб.) и в 1982 году в Горьком. Появление первых компьютерных преступлений в начале 80-х годов и дальнейший рост компьютерной преступности были в основном обусловлены переходом

[107] Долгиева М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. — 2018. — № 11. — С. 106.

на автоматизированные системы документооборота[108]. Использование иностранных терминов является причиной возникновения сложной проблемы их перевода на русский юридический язык.

В силу трансграничности правонарушений огромное значение приобретают международные договоры. Важнейшим из них является *Конвенция о преступности в сфере компьютерной информации* от 23 ноября 2001 года. Целью принятия данного документа является гармонизация национального законодательства в сфере компьютерных преступлений путем (1) приведения правового закрепления преступлений, связанных с компьютерами, к единообразию в национальных законодательствах стран; (2) сближения национальных уголовно-процессуальных норм и (3) организации международного сотрудничества по предотвращению и расследованию компьютерных преступлений.

Самое важное в главе 3

1. Функциональным назначением института риска является возможность устанавливать правила, позволяющие свести к минимуму возможные вредоносные последствия негативных действий и явлений, или, в случае невозможности их избежать, распределять убытки между участниками экономического оборота.

2. Под угрозой экономической безопасности понимается совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба.

3. Одной из самых серьезных угроз общественным отношениям являются иностранные социальные сети. Задачей законодателя является создание эффективной системы нормативных актов, минимизирующих или ликвидирующих эти угрозы.

4. Наиболее частыми нарушениями в социальных сетях являются (1) использование двойных стандартов при оценке событий в России и в западных странах; (2) размещение информации, направленной на нарушение территориальной целостности России и (3) нарушения прав российских граждан.

---

[108] Криминология. Учебник / под. ред. А. И. Долговой. — М.: Изд-во «Норма», 2005. — С. 76.

5. Угроза личной жизни гражданина существовала всегда, но с появлением *автоматизированной обработки данных об индивидах* она резко усилилась. Именно для минимизации этих угроз была разработано понятие «персональные данные». Под ним понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.

6. Правонарушения в сфере цифровых отношений представляется возможным квалифицировать на (1) классические, которые прямо упомянуты в российских нормативных актах (например, хищение, мошенничество и т. д.) и (2) специальные нарушения, для наименования которых используются, как правило, термины, реципированные из иностранных нормативных актов (кардинг, спаминг, фишинг, DDoS-атаки и т. д.).

Вопросы

1. Функциональное назначение категории риск.
2. Различие риска в экономическом и юридическом понимании.
3. Юридическое определение социальной сети.
4. Классификация правонарушений в сфере цифровых отношений.
5. Понятие принципа двойной криминализации деяния.

Литература

1. Белгородцева Н. Г. Теоретико-правовые аспекты защиты персональных данных: дис. ... канд. юрид. наук. — М., 2012.

2. Бураева Л. А. Социальные сети как угроза информационной безопасности // Пробелы в российском законодательстве. — 2017. — № 3. — С. 71–73.

3. Долгиева М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. — 2018. — № 11. — С. 103–108.

4. Попов Е. В., Семячков К. А. Проблемы экономической безопасности цифрового общества в условиях глобализации // Экономика региона. — 2018. — Т. 14. — Вып. 4. — С. 1088–1101.

5. Перчаткина С. А. и др. Социальные интернет-сети: правовые аспекты // Журнал российского права. — 2012. — № 5. — С. 14–24.

Особенная часть

Глава 4. Уголовно-правовая ответственность за правонарушения в цифровой сфере

4.1. Уголовная политика в экономической сфере и особенности обеспечения экономической безопасности нормами уголовного права

Концепция уголовно-правовой политики Российской Федерации представляет собой систему официально принятых в государстве положений, определяющих сущность, цель, направления, приоритеты и критерии эффективности нормотворческой и правоприменительной деятельности в области защиты личности, общества и государства от преступных посягательств средствами уголовного законодательства[109]. Согласно пункту 2 данного документа, уголовно-правовая политика выступает одним из направлений реализации государственной стратегии обеспечения криминологической безопасности. В настоящее время идет процесс формирования нового научного направления — экономической криминологии и ее составной части — криминологии экономической безопасности[110]. Очевидно, что в криминологию экономической безопасности необходимо включить криминологию цифровой безопасности.

Важность данной проблемы обусловило включение в состав важнейших показателей состояния экономической безопасности *уровень преступности в сфере экономики* (Стратегии экономической безопасности Российской Федерации на период до 2030 года).

---

[109] Концепция уголовно-правовой политики Российской Федерации. Разработана Общественной палатой Российской Федерации // https://www.oprf.ru/ru/discussions/1389/newsitem

[110] Егоршин В. М. Экономическая преступность и безопасность современной России (теоретико-криминологический анализ). Дис. ... д-ра юрид. наук. — СПб., 2000. — С. 34.

Уголовное право имеет по отношению к экономике, производству не прямую роль регулятора, но выполняет охранительную функцию; уголовно-правовой механизм включается тогда, когда не срабатывают иные (цивилистические, административные) инструменты правового воздействия[111].

4.2. Понятие и общая характеристика преступления

4.2.1. Основанием уголовной ответственности является *преступление*. Оно устанавливается только Уголовным кодексом РФ, в отличие, например, от административной ответственности, которая может быть установлена не только в Кодексе об административных правонарушениях РФ, но и в других законах и подзаконных актах.

Под *преступлением* понимается общественно опасное, запрещенное уголовным законом, виновное и наказуемое волевое действие или бездействие (ст. 14 Уголовного кодекса РФ).

Важнейшим признаком преступления является *общественная опасность*. Квалификация преступления как угрозы общественным отношениям означает, что какое-либо действие или бездействие причинить им вред или создает угрозу причинения вреда.

Согласно статье 15 Уголовного кодекса РФ, в зависимости от характера и степени общественной опасности, незаконные деяния подразделяются на *преступления небольшой тяжести* (максимальное наказание не превышает трех лет лишения свободы), *преступления средней тяжести* (наказание до десяти лет лишения свободы), *тяжкие преступления* (умышленные деяния, за совершение которых установлено наказание до десяти лет лишения свободы, и неосторожные деяния — до пятнадцати лет лишения свободы) и *особо тяжкие преступления* (умышленные деяния, за совершение которых установлено наказание свыше десяти лет или более строгое наказание).

Для того чтобы какое-либо деяние было признано преступлением необходимо наличие 4 элементов (состав преступления):

1. Объект преступления — социальная ценность, которая защищается от преступных посягательств.

---

[111] Александрова И. А. Современная уголовная политика по обеспечению экономической безопасности и противодействию коррупции. Дис. ... д-ра юрид. наук. — Н. Новгород, 2015. — С. 208.

2. Объективная сторона — акт внешнего поведения человека, выраженный в действие или бездействие.

3. Субъект преступления — лицо, совершившее преступление.

4. Субъективная сторона — психическая деятельность субъекта в момент совершения им преступления.

4.3. Общее и особенное экономических преступлений

Легитимного определения экономического преступления не существует. В литературе принято различать две разные группы экономических преступлений: первая образуется преступлениями, которые всегда безоговорочно, часто в силу прямого указания закона, совершаются по экономической мотивации; вторая включает в себя преступления, для которых экономическая мотивация не является обязательным признаком состава, однако она вполне возможна. Первая группа может быть названа безусловно экономическими преступлениями, вторая — ситуативными экономическими преступлениями.

Принято выделять следующие *признаки экономических преступлений*:

1. Осуществление в сфере предпринимательства, в сфере бизнеса под прикрытием законной экономической деятельности.

2. Осуществление непосредственно в процессе экономической (предпринимательской) деятельности, в ее границах и пределах компетенции.

3. Осуществление субъектами предпринимательской деятельности.

4. Использование криминальных методов присвоения экономических благ в процессе осуществления законной экономической деятельности, паразитирование на хозяйственно-правовых условиях, воспроизводимых официальной (разрешенной) рыночной экономической средой.

5. Высокий социальный статус страты предпринимателей и высокий кредит доверия к ней со стороны общества, которые проституируются бизнесменами-делинквентами, служат им прикрытием для осуществления своей преступной деятельности.

6. Анонимность, отсутствие персонификации жертв.

7. Отсутствие прямого контакта с жертвой.

8. Специфичность и множественность объектов посягательств.

9. Специфичность субъектов экономической преступности.

10. Массовость и типичность преступлений.

11. Скрытность преступлений.

12. Корыстный характер преступлений.

13. Отношение к категории ненасильственных преступлений.

14. Наличие феномена безразличного, индифферентного отношения общества к экономической преступности[112].

Особенностью состава большинства экономических преступлений является то, что они формируются при помощи *бланкетных норм* Уголовного кодекса РФ, так как состав многих преступлений обставляется еще известными юридическими фактами, предположения, вытекающими из положений норм самых разных отраслей права. Так, например, в статье 171 УК РФ содержится санкция за незаконную предпринимательскую деятельность. Однако определения данного понятия нет. Поэтому при толковании данной нормы необходимо использовать признаки предпринимательской деятельности, содержащиеся в гражданском законодательстве.

4.4. Преступления в цифровой сфере

Преступления в цифровой сфере именуются *преступлениями в сфере компьютерной информации*. В настоящее они закреплены в следующих трех статьях одноименной главы Уголовного кодекса РФ:

1) неправомерный доступ к компьютерной информации (статья 272);

2) создание, использование и распространение вредоносных компьютерных программ (статья 273);

---

[112] Колесников В. В. Экономическая преступность в современном рыночном хозяйстве // Криминология-XX век. — М.: Юридический центр Пресс, 2000. — С. 334.

3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274)[113].

Неправомерный доступ к компьютерной информации (статья 272 Уголовного кодекса РФ). *Объектом преступления* являются общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. *Дополнительный объект преступления* — общественные отношения, обеспечивающие интересы службы (часть 3 статьи 272 Уголовного кодекса РФ).

Объективной стороной данного состава преступления является неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. При этом следует учитывать *широкое понимание содержания объективной стороны — в нее включают также неправомерный доступ к устройству, не подпадающему под определение электронно-вычислительной машины, но по своим свойствам и функциям фактически не уступающему электронно-вычислительной машине по возможности хранения и обработки информации*. Таковыми в настоящее время являются, например, мобильные телефоны и смартфоны[114].

Состав данного *преступления* является материальным и предполагает наличие одного из нижеследующих фактов:

а) уничтожение информации — это приведение информации или ее части в непригодное для использования состояние

---

[113] «В литературе также применяется термин «киберпреступность», под которым понимается родовое понятие, охватывающее как компьютерную преступность в узком значении этого слова (где компьютер является предметом, а информационная безопасность — объектом преступления), так и иные посягательства, где компьютеры используются как орудия или средства совершения преступлений» / Глушков А. В. Проблемы правового регулирования интернет-отношений. Автореф. дис. … канд. юрид. наук. — СПб., 2007. — С. 19.

[114] Нет необходимости указывать в диспозиции рассматриваемой статьи все объекты обращения цифровой информации, в том числе и беспроводные, целесообразно лишь определить их как информационно-телекоммуникационные устройства, их системы и сети, что соответствовало бы современному состоянию научно-технического прогресса и устоявшемуся понятийному аппарату / Бегишев И. Р. Преступления в сфере обращения цифровой информации // Информационное право. — 2010. — № 2. — С. 14.

независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени;

б) блокирование информации — результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации — внесение изменений в компьютерную информацию. Законом установлены случаи легальной модификации программ лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

г) копирование информации — создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме — от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т. п.[115]

Субъективная сторона преступления — вина в форме прямого или косвенного умысла или неосторожности.

Субъект преступления — общий, то есть любое вменяемое лицо, достигшее шестнадцати лет. Однако исключение предусмотрено для части 3 статьи 272 Уголовного кодекса РФ.

---

[115] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утв. Генпрокуратурой России // www.genproc.gov.ru.

В ней предусматривается наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения.

Создание, **использование и распространение вредоносных компьютерных программ** (статья 273 Уголовного кодекса РФ). *Объектом преступления* являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Объективная сторона преступления сконструирована альтернативно: (1) создание программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты; (2) распространение этих программ или машинных носителей с такими программами или (3) использовании вышеуказанных программ или машинных носителей.

Состав преступления является формальным[116]. Преступление является оконченным с момента (1) создания; (2) использования или (3) распространения этих программ или информации, создающих угрозу наступления указанных в законе последствий.

Субъективная сторона состава преступления характеризуется виной в виде прямого умысла.

Субъект преступления общий, то есть любое вменяемое лицо, достигшее шестнадцати лет.

Квалифицирующими признаками статей 272 и 273 Уголовного кодекса РФ являются наступление тяжких последствий совершенных деяний или угроза наступления таких последствий. Как указано в Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, тяжесть последствий должна определяться с учетом всей совокупности обстоятельств дела — причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф,

[116] Составы преступлений классифицируются на материальные и формальные. Для *материальных составов* характерно наступление конкретных общественно опасных последствий. В *формальных* же *составах* наступление этих последствий не является обязательным для привлечения к ответственности.

причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и другие[117].

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 Уголовного кодекса РФ). *Основным объектом преступления* являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации, *дополнительным* — общественные отношения, обеспечивающие в зависимости от характера последних, иные значимые социальные ценности (жизнь человека, здоровье многих людей, собственную безопасность и т. п.).

Предметом данного преступления являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

Объективная сторона преступления состоит в нарушении правил хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если такое нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Субъективная сторона данного состава преступления включает две формы вины — умысел и неосторожность. *Субъект* общий.

Установлены *квалифицирующие признаки* — тяжкие последствия или создание угрозы их наступления.

Самое важное в главе 4

1. Под преступлением понимается общественно опасное, запрещенное уголовным законом, виновное и наказуемое волевое

[117] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утв. Генпрокуратурой РФ // ИПБ КонсультантПлюс.

действие или бездействие. Для того чтобы какое-либо деяние было признано преступлением необходимо наличие четырех элементов (состав преступления): объект преступления, объективная сторона, субъект преступления — лицо, совершившее преступление и субъективная сторона.

2. Особенностью состава большинства преступлений в цифровой сфере является то, что они формируются при помощи бланкетных норм Уголовного кодекса РФ, так как состав многих преступлений обставляется еще известными юридическими фактами, предположения, вытекающими из положений норм самых разных отраслей права.

3. Преступления в цифровой сфере именуются преступлениями в сфере компьютерной информации. В настоящее они закреплены в следующих трех статьях одноименной главы Уголовного кодекса РФ: неправомерный доступ к компьютерной информации (статья 272), создание, использование и распространение вредоносных компьютерных программ (статья 273) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274).

Вопросы

1. Функциональное назначение Концепции уголовно-правовой политики Российской Федерации.

2. В чем выражается охранительная функция уголовного права?

3. Основные признаки экономических преступлений.

4. В чем состоит специфика цифровых преступлений?

Литература

1. Алиев В. М. Политико-правовые аспекты перехода к цифровой экономике в России // Российский следователь. — 2018. — № 9. — С. 48–52.

2. Безверхов А. Г., Григорян Г. Р. Корыстные преступления против собственности в условиях цифровой трансформации // Российская юстиция. — 2021. — № 1. — С. 16–17.

3. Григорян Г. Р. О социально-правовой сущности корыстных имущественных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Российская юстиция. — 2020. — № 10. — С. 13–15.

4. Денисов Н. Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом // Международное уголовное право и международная юстиция. — 2019. — № 4. — С. 18–20.

5. Дремлюга Р. И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. — 2018. — № 4. — С. 52–57.

6. Долгиева М. М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. — 2018. — № 10. — С. 109–115.

7. Решняк М. Г., Борисов С. В. Современные проблемы формирования уголовно-правовой основы противодействия преступлениям в сфере цифровой экономики // Безопасность бизнеса. — 2020. — № 3. — С. 41–45.

8. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. — М.: Инфра-М, 2019.

9. Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. — М.: Статут, 2016.

Глава 5. Административно-правовая ответственность за правонарушения в цифровой сфере

5.1. Понятие и общая характеристика административно-правового регулирования

Административное право представляет собой систему правовых норм, регулирующих отношения в сфере государственного и муниципального управления. Соответственно, административное право, как самостоятельная *отрасль права* (1) определяет порядок совершения управленческих действий и соответствующих управленческих процедур; (2) гарантирует общественный порядок и общественную безопасность; (3) устанавливает виды административного принуждения за отрицательные результаты управления, неисполнение или ненадлежащее исполнение должностных обязанностей, а также ответственность за совершение правонарушений в различных областях управления и (4) обеспечивает права, свободы и законные интересы как граждан, так и юридических лиц[118].

2.1.2. Административно-правовым отношениям свойственны следующие *признаки*:

1) они возникают, по общему правилу, между властвующим и подчиненным субъектами. Поэтому управленческие акты приобретают юридическую силу независимо от согласия подчиненного.

Согласно обоснованному мнению Ю. А. Тихомирова, «административно-правовое регулирование в качестве разновидности

---

[118] См. напр.: Ордина О. Н. К вопросу о понимании предмета административного права // Административное право и процесс. — 2020. — № 12. — С. 18; Сигаева А. А., Мальцева А. Ю. Задачи административного права как отрасли права и ее общественное значение // Актуальные проблемы совершенствования законодательства и правоприменения. Сборник материалов VI Внутривузовского круглого стола. — 2020. — С. 131; Старилов Ю. Н. Административное право: в 2 ч. — Воронеж: Изд-во Воронежского гос. университета, 1988. — Ч. 1: История. Наука. Предмет. Нормы. — С. 286; Тамбовцева С. Б. Административное право в контексте российского права // Молодой ученый. — 2021. — № 16 (358). — С. 300–301 и др.

государственного регулирования есть механизм императивно-нормативного упорядочения организации и деятельности субъектов и объектов управления и формирования устойчивого правового порядка их функционирования. Оно сочетается с нормами гражданского и налогового законодательства и чаще всего как бы «оформляет», «поглощает», «вводит» их в действие в том или ином цикле и ситуации жизнедеятельности регулируемых объектов»[119];

2) административно-правовые отношения складываются преимущественно в сфере государственного управления;

3) в сфере административно-правовых отношений права и обязанности, как правило, не разделены: *право является обязанностью*, *а обязанность — правом*.

Сложность общественных отношений, регулируемых нормами административного права, обусловила усложнение административно-правовых отношений. Соответственно, правовую категорию «режимное административно-правовое регулирование» можно определить как систему, объединяющую в себе различные правовые средства, образуемую для урегулирования сложных многосубъектных, многоуровневых отношений, для достижения гарантированного правового результата, объединяющую в себе методы правового регулирования различных отраслей права, имеющую ярко выраженную императивную направленность, устанавливающую правовые статусы субъектов и объектов правоотношений, режимные правила их поведения или функционирования, а также гарантии реализации правовых статусов субъектов и объектов правоотношений и режимных правил[120].

Административным правонарушением является противоправное, виновное действие или бездействие физического или юридического лица, за которое федеральными или региональными законами об административных правонарушениях установлена административная ответственность.

За одни и те же деяния может быть предусмотрена как административная, так и уголовная ответственности. Так,

---

[119] Тихомиров Ю. А. Административное право и процесс: полный курс. — М., 2015. — С. 360.

[120] Долгополов А. А. Сущность режимного административно-правового регулирования // Административное право и процесс. — 2012. — № 1. — С. 18–22.

например, уклонение от уплаты налогов может квалифицироваться как административный проступок, так и преступление, то есть деяние, предусмотренное Уголовным кодексом РФ. Административные проступки и преступления отличаются степенью общественной опасности. Административная ответственность наступает за правонарушения только в том случае, если они по своему характеру не влекут за собой уголовной ответственности.

Основанием наступления *административной ответственности* является совершение субъектом административного правонарушения, при условии, что оно обладает всеми признаками правонарушения (противоправность, виновность, наказуемость).

Состав административного проступка, также как и преступления, включает в себя четыре элемента: объект, объективная сторона, субъект и субъективная сторона.

Объектом правонарушения является система правоотношений, охраняемых законодательством об административных правонарушениях.

Объективной стороной правонарушения является акт внешнего поведения субъекта — действие или бездействие.

Субъектом правонарушения может быть как физическое, так и юридическое лицо.

Субъективная сторона совершения административного правонарушения характеризует психическое переживание лица по поводу совершенного им деяния.

Административное правонарушение может быть совершено как *умышленно*, так и *не умышленно*. Умышленная вина носит социально более опасный характер, нежели неосторожная вина, так как лицо осознает и осознавало, что совершает противоправное деяние. Совершение деяния по неосторожности может служить основанием для назначения менее строгого наказания.

Виды административных правонарушений. Критерием деления административных правонарушений на виды является родовой объект, т. е. общественные отношения в конкретной области государственной и общественной жизни, государственного управления.

На основе данного критерия можно выделить следующие виды административных правонарушений:

1. Административные правонарушения, посягающие на права граждан (глава 5, ст. 5.1–5.44). К ним, в частности, относятся: нарушение права гражданина на ознакомление со списком избирателей, участников референдума; вмешательство в работу избирательной комиссии, комиссии референдума; неисполнение решения избирательной комиссии, комиссии референдума; нарушение порядка предоставления списков избирателей, участников референдума или сведений об избирателях, участниках референдума; незаконное использование денежных средств кандидатом, зарегистрированным кандидатом, избирательным объединением, избирательным блоком, инициативной группой по проведению референдума и др.

2. Административные правонарушения, посягающие на здоровье, санитарно-эпидемиологическое благополучие населения и общественную нравственность (глава 6, ст. 6.1–6.14). Они включают, в частности: незаконное занятие частной медицинской практикой, частной фармацевтической деятельностью либо народной медициной; незаконное приобретение либо хранение наркотических средств или психотропных веществ, а также оборот их аналогов; потребление наркотических средств или психотропных веществ без назначения врача; получение дохода от занятия проституцией, если этот доход связан с занятием другого лица проституцией, и ряд других.

3. Административные правонарушения в области охраны собственности (глава 7, ст. 7.1–7.28). Это, в частности: самовольное занятие земельного участка; уничтожение специальных знаков; нарушение авторских и смежных прав, изобретательских и патентных прав; нарушение требований сохранения, использования и охраны объектов культурного наследия (памятников истории и культуры) федерального значения, их территорий и зон их охраны и др.

4. Административные правонарушения в области охраны окружающей природной среды и природопользования (глава 8, ст. 8.1–8.40). Эти правонарушения, в частности, включают: несоблюдение экологических требований при планировании, технико-экономическом обосновании проектов, проектировании, размещении, строительстве, реконструкции, вводе

в эксплуатацию, эксплуатации предприятий, сооружений или иных объектов; несоблюдение экологических и санитарно-эпидемиологических требований при обращении с отходами производства и потребления или иными опасными веществами; сокрытие или искажение экологической информации; порча земель; нарушение требований по рациональному использованию недр и др.

5. Административные правонарушения в промышленности, строительстве и энергетике (глава 9, ст. 9.1–9.14). К ним, в частности, относятся: нарушение требований промышленной безопасности или условий лицензий на осуществление видов деятельности в области промышленной безопасности опасных производственных объектов; нарушение норм и правил безопасности гидротехнических сооружений; нарушение требований нормативных документов в области строительства; нарушение правил использования атомной энергии и учета ядерных материалов и радиоактивных веществ и ряд других.

6. Административные правонарушения в сельском хозяйстве, ветеринарии и мелиорации земель (глава 10, ст. 10.1–10.14). Это, в частности, нарушение правил борьбы с карантинными, особо опасными и опасными вредителями растений, возбудителями болезней растений, растениями-сорняками; нарушение ветеринарно-санитарных правил перевозки или убоя животных, правил переработки, хранения или реализации продуктов животноводства; сокрытие сведений о внезапном падеже или об одновременных массовых заболеваниях животных; проведение мелиоративных работ с нарушением проекта и др.

7. Административные правонарушения на транспорте (глава 11, ст. 11.1–11.29). Они, в частности, включают такие правонарушения, как: действия, угрожающие безопасности движения на железнодорожном транспорте; действия, угрожающие безопасности движения на железнодорожном транспорте; нарушение правил использования воздушного пространства; действия, угрожающие безопасности движения на водном транспорте; нарушение правил эксплуатации судов, а также управление судна лицом, не имеющим права управления, и ряд других.

8. Административные правонарушения в области дорожного движения (глава 12, ст. 12.1–12.36). К ним относятся, в частности, такие правонарушения, как: управление транспортным

средством, не зарегистрированным в установленном порядке; управление транспортным средством с нарушением правил установки на нем государственных регистрационных знаков; управление транспортным средством водителем, не имеющим при себе документов, предусмотренных Правилами дорожного движения; нарушение правил установки на транспортном средстве устройств для подачи специальных световых или звуковых сигналов; управление транспортным средством при наличии неисправностей или условий, при которых эксплуатация транспортных средств запрещена; нарушение правил применения ремней безопасности или мотошлемов; превышение установленной скорости движения и другие правонарушения в данной области.

9. Административные правонарушения в области связи и информации (глава 13, ст. 13.1–13.24). Это, в частности: самовольные установка или эксплуатация узла проводного вещания; самовольное подключение к сети электрической связи оконечного оборудования; нарушение правил охраны линий или сооружений связи; использование несертифицированных средств связи либо предоставление несертифицированных услуг связи и ряд других.

10. Административные правонарушения в области предпринимательской деятельности (глава 14, ст. 14.1–14.25). К данному виду относятся, в частности, следующие правонарушения: осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии); незаконная продажа товаров (иных вещей), свободная реализация которых запрещена или ограничена; нарушение законодательства о рекламе; продажа товаров, выполнение работ либо оказание населению услуг ненадлежащего качества или с нарушением санитарных правил; продажа товаров, выполнение работ либо оказание услуг при отсутствии установленной информации либо без применения контрольно-кассовых машин; обман потребителей и другие правонарушения.

11. Административные правонарушения в области финансов, налогов и сборов, рынка ценных бумаг (глава 15, ст. 15.1–15.26). Этот вид правонарушений включает в себя, в частности, такие правонарушения, как: нарушение сроков представления налоговой декларации; непредставление сведений, необходимых

для осуществления налогового контроля; нарушение порядка работы с денежной наличностью и порядка ведения кассовых операций; невыполнение обязанностей по контролю за соблюдением правил ведения кассовых операций; нарушение срока постановки на учет в налоговом органе и ряд других.

12. Административные правонарушения в области таможенного дела (нарушения таможенных правил) (глава 16, ст. 16.1–16.22). Это, в частности: незаконное перемещение товаров и (или) транспортных средств через таможенную границу Российской Федерации; перемещение товаров и (или) транспортных средств с несоблюдением мер по защите экономических интересов Российской Федерации и других запретов и ограничений; неуведомление при ввозе товаров и (или) транспортных средств о пересечении таможенной границы Российской Федерации; нарушение режима зоны таможенного контроля и другие правонарушения.

13. Административные правонарушения, посягающие на институты государственной власти (глава 17, ст. 17.1–17.13). К ним, в частности, относятся: невыполнение законных требований члена Совета Федерации или депутата Государственной Думы, воспрепятствование деятельности Уполномоченного по правам человека в Российской Федерации, неисполнение распоряжения судьи или судебного пристава, воспрепятствование явке в суд народного или присяжного заседателя, невыполнение законных требований прокурора, следователя, дознавателя или должностного лица, осуществляющего производство по делу об административном правонарушении, незаконные действия по отношению к государственным символам Российской Федерации, а также ряд других правонарушений в данной области.

14. Административные правонарушения в области защиты Государственной границы Российской Федерации и обеспечения режима пребывания иностранных граждан или лиц без гражданства на территории Российской Федерации (глава 18, ст. 18.1–18.14). Среди правонарушений данного вида можно назвать, в частности, нарушение режима Государственной границы Российской Федерации; нарушение пограничного режима в пограничной зоне; нарушение пограничного режима в территориальном море и во внутренних морских водах Российской

Федерации; нарушение режима в пунктах пропуска через Государственную границу Российской Федерации, а также другие правонарушения в данной области.

15. Административные правонарушения против порядка управления (глава 19, ст. 19.1–19.25). Это, в частности: самоуправство, умышленное повреждение или срыв печати (пломбы); неповиновение законному распоряжению сотрудника милиции, военнослужащего либо сотрудника органов уголовно-исполнительной системы; неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль); невыполнение в срок законного предписания (постановления, представления) органа (должностного лица), осуществляющего государственный надзор (контроль); непредставление сведений (информации), а также другие правонарушения.

16. Административные правонарушения, посягающие на общественный порядок и общественную безопасность (глава 20, ст. 20.1–20.27). К ним относятся, в частности: мелкое хулиганство; нарушение установленного порядка организации либо проведение собрания, митинга, демонстрации, шествия или пикетирования; пропаганда и публичное демонстрирование нацистской атрибутики или символики; нарушение требований пожарной безопасности; нарушение требований режима чрезвычайного положения; нарушение правил производства, продажи, коллекционирования, экспонирования, учета, хранения, ношения или уничтожения оружия и патронов к нему; стрельба из оружия в не отведенных для этого местах, а также ряд других.

17. Административные правонарушения в области воинского учета (глава 21, ст. 21.1–21.7). Это, в частности: непредставление в военный комиссариат или в иной орган, осуществляющий воинский учет, списков граждан, подлежащих первоначальной постановке на воинский учет; неоповещение граждан о вызове их по повестке военного комиссариата или иного органа, осуществляющего воинский учет; неисполнение гражданами обязанностей по воинскому учету; уклонение от медицинского обследования; умышленные порча или утрата документов воинского учета, а также другие правонарушения[121].

[121] См. напр.: Воронцова А. А. Административная ответственность // СПС КонсультантПлюс, 2021; Закопырин В. Н., Павлова Л. В. Концептуальные

5.2. Административная ответственность за правонарушения в цифровой сфере

Для административных проступков в сфере цифровых отношений характерна, также и для преступлений, высокая роль *бланкетных норм*.

Так же, как и в случае уголовной ответственности, *в законодательстве о наказаниях за административные проступки еще нет специальных норм о цифровых правонарушениях*. Поэтому применяются (1) общие нормы административного законодательства (мошенничество, нарушение авторских и смежных прав, изобретательских и патентных прав, нарушение законодательства о рекламе и т. д.) и (2) нормы информационного законодательства (например, нормы главы 13 Кодекса об административных правонарушениях РФ «Административные правонарушения в области связи и информации»).

К числу *распространенных информационных правонарушений* относятся:

– нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (статья 13.11 Кодекса об административных правонарушениях РФ);

– нарушение правил защиты информации (статья 13.12 Кодекса об административных правонарушениях РФ);

– незаконная деятельность в области защиты информации (статья 13.13 Кодекса об административных правонарушениях РФ);

– разглашение информации с ограниченным доступом (статья 13.14 Кодекса об административных правонарушениях РФ);

– воспрепятствование уверенному приему радио- и телепрограмм и работе сайтов в сети «Интернет» (статья 13.18 Кодекса об административных правонарушениях РФ);

– неисполнение обязанностей организатором распространения информации в сети «Интернет» (статья 13.31 Кодекса об административных правонарушениях РФ).

положения двухуровневой административной ответственности в проекте нового КоАП РФ: быть или не быть? // Административное право и процесс. — 2020. — № 10. — С. 38–40; Кисин В. Р. Некоторые суждения по поводу Концепции нового Кодекса Российской Федерации об административных правонарушениях // Административное право и процесс. — 2020. — № 2. — С. 37–42 и др.

Нарушение законодательства Российской Федерации в области персональных данных (статья 13.11 Кодекса об административных правонарушениях РФ). Одним из негативных последствий интенсификации инновационного развития страны и, соответственно, расширения использования искусственного интеллекта, облачных технологий, технологий больших данных, Интернета вещей и других информационных технологий, является *усиление угрозы доступа к информации о личной жизни граждан и ее неправомерного использования*. Законодатель, осознавая серьезность данной тенденции, был вынужден разработать систему нормативных актов, обеспечивающих минимизацию этих угроз. Базовое положение, содержащееся в статье 23 Конституции РФ, конкретизировано системой нормативных актов, важнейшими из которых, очевидно, являются федеральный закон «О персональных данных», Трудовой кодекс РФ и ряд других законов.

Основой отечественного законодательства в сфере персональных данных являются международные договоры, важнейшим из которых является Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.

Очевидно, что угроза личной жизни гражданина существовала всегда, но с появлением *автоматизированной обработки данных об индивидах* она резко усилилась. Согласно обоснованному мнению одного из специалистов, с появлением автоматизированной обработки персональных данных и их размещением в открытых информационных сетях ситуация изменилась: возникла возможность несанкционированного использования баз данных, в том числе и в криминальных целях, то есть опасность нежелательного для гражданина разглашения конфиденциальной информации[122]. Именно для минимизации этих угроз была разработано понятие «персональные данные».

1. *Объектом правонарушения* являются общественные отношения, складывающиеся в области защиты информации.

2. *Объективная сторона* — обработка персональных данных с нарушением установленных требований.

---

[122] Белгородцева Н. Г. Теоретико-правовые аспекты защиты персональных данных / дис. … канд. юрид. наук. — М., 2012. — С. 98.

Обработка персональных данных допускается при соблюдении следующих требований:

1) по общему правилу необходимо наличие согласия субъекта персональных данных на обработку его персональных данных;

2) если обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

3) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных федеральным законом «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при

условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста или законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Субъект правонарушения — общий. *Субъективная сторона* — умысел или неосторожность.

Нарушение правил защиты информации (статья 13.12 Кодекса об административных правонарушениях РФ). *Объектами правонарушений* являются общественные отношения по защите информации. Правила обеспечения защиты в настоящее время урегулированы Гражданским кодексом РФ, федеральным законом «О персональных данных», федеральным законом «Об информации, информационных технологиях и о защите информации», федеральным законом «О коммерческой тайне», федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», указом Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» и рядом других нормативных актов.

Объективная сторона правонарушения выражается в следующих действиях:

1) нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации;

2) использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации;

3) нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и оказанием услуг по защите информации, составляющей государственную тайну;

4) использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну;

5) грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации;

6) нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

7) нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие деяния не содержат уголовно наказуемого деяния.

3. *Субъектами* правонарушения являются граждане, должностные лица и организации.

4. *Субъективная сторона* правонарушения характеризуется умыслом или неосторожностью.

Незаконная деятельность в области защиты информации (статья 13.13 Кодекса об административных правонарушениях РФ). *Объектом* проступка являются общественные отношения в области защиты информации.

Порядок защиты информации регламентирован федеральным законом «Об информации, информационных технологиях и о защите информации», федеральным законом «О федеральной службе безопасности» и другими нормативными актами.

Объективную сторону правонарушения составляют занятие видами деятельности в области защиты информации без получения в установленном порядке специального разрешения.

Субъективной стороной является умышленное или по неосторожное нарушение установленных правил получения разрешения на соответствующий вид деятельности. *Субъект* — общий.

Неисполнение обязанностей организатором распространения информации в сети «Интернет» (статья 13.31 Кодекса об административных правонарушениях РФ). *Объектом* проступка являются общественные отношения в сфере информации и информационных технологий. *Объективная сторона* проступка включает в себя следующие альтернативные действия:

1) неисполнение организатором распространения информации в сети Интернет обязанности уведомить компетентный орган о начале осуществления деятельности по обеспечению функционирования информационных систем и программ для электронных вычислительных машин пользователей сети Интернет;

2) неисполнение организатором распространения информации обязанности хранить и предоставлять компетентному органу информацию о фактах приема, передачи, доставки и обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию о таких пользователях;

3) неисполнение организатором распространения информации в сети Интернет обязанности обеспечивать реализацию требований к оборудованию и программно-техническим средствам, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Субъективная сторона представляет собой умысел. *Субъект* — общий.

Воспрепятствование работе сайтов в сети «Интернет» (пункт 2 статьи 13.18 Кодекса об административных правонарушениях РФ). *Объектом проступка* является, в частности, нормальное функционирование сайтов в сети Интернет.

Объективная сторона включает в себя (1) воспрепятствование работе сайтов в сети Интернет и (2) совершение действий, направленных на заведомо незаконное ограничение доступа к таким сайтам.

Субъект правонарушения является общим. *Субъективная сторона* характеризуется умыслом.

Самое важное в главе 5

1. Административным правонарушением является противоправное, виновное действие или бездействие физического или юридического лица, за которое федеральными или региональными законами об административных правонарушениях установлена административная ответственность.

2. Для административных проступков в сфере цифровых отношений характерна, также и для преступлений, высокая роль бланкетных норм. В законодательстве о наказаниях за административные проступки еще нет специальных норм о цифровых правонарушениях. Поэтому применяются нормы информационного законодательства и общие нормы административного законодательства, например, мошенничество, нарушение авторских и смежных прав, изобретательских и патентных прав, нарушение законодательства о рекламе и т. д.

Вопросы

1. Предмет и метод административного права как отрасли российского права.

2. Система административного права.

3. Нормы административного права: понятия, виды, структура. Административно-правовые отношения: понятие, признаки, виды.

4. Понятие административного правонарушения.

5. Объективная сторона неисполнения обязанностей организатором распространения информации в сети «Интернет».

Литература

1. Балытников В. В., Новиков А. В. Проблемы регламентации и применения административной ответственности за распространение информационных материалов, содержащих изображения запрещенной символики и атрибутики // Административное право и процесс. — 2016. — № 10. — С. 40–44.

2. Гурин О., Полянский А. Об электронной подписи и административной ответственности // Прогосзаказ.рф. — 2020. — № 10. — С. 6–17.

3. Елфимова Е. В., Коркин А. В., Гришаков А. Г. Административно-правовой механизм обеспечения экономической безопасности: теоретический аспект // Алтайский юридический вестник. — 2020. — № 4 (32). — С. 39–46.

4. Елфимова Е. В., Коркин А. В. Административное принуждение как средство обеспечения экономической безопасности / Экономико-правовые проблемы обеспечения экономической безопасности. Материалы Всероссийской научно-практической конференции / отв. за вып. Е. Г. Анимица, Г. З. Мансуров. — 2018. — С. 199–203.

5. Зеленцов А. Б., Натрошвили Г. И. Цифровое обеспечение административного правосудия в условиях построения «электронного государства»: некоторые теоретические вопросы // Административное право и процесс. — 2020. — № 12. — С. 24–28.

6. Зубарев С. М., Сладкова А. В. О понятии и сущности цифровых технологий контроля в сфере государственного управления // Административное право и процесс. — 2019. — № 9. — С. 53–59.

7. Коркин А. В. и др. Административное право. Учебник. — М., 2011.

8. Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. — 2017. — № 1. — С. 17–21.

9. Попов Л. Л. Развитие теории административного права в современных условиях // Административное право и процесс. — 2020. — № 7. — С. 20–24.

10. Тиунова Н. В. Некоторые проблемные аспекты осуществления государственного контроля и привлечения к административной ответственности за нарушения прав покупателей несанкционированными и обезличенными интернет-магазинами в России // Пермский юридический альманах. Ежегодный научный журнал. — 2019. — № 1. — С. 152–162.

11. Чаннов С. Е. Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. — 2018. — № 9. — С. 48–54.

Глава 6. Гражданско-правовая ответственность за правонарушения в цифровой сфере

6.1. Понятие и функции гражданского права. Специфика обеспечения экономической безопасности нормами гражданского права

3.1.1. Гражданское право является наиболее близкой к экономике отраслью права. По этой причине его иногда именуют экономическим правом. Как и любая отрасль права, гражданское право имеет свой предмет и метод регулирования. Согласно статье 2 Гражданского кодекса РФ, нормы гражданского права регулируют следующие виды отношений:

1) имущественные отношения равноправных субъектов;

2) личные неимущественные отношения, не связанные с имущественными;

3) корпоративные отношения (внутриорганизационные отношения);

4) личные неимущественные отношения, связанные с имущественными (по поводу результатов творческой деятельности).

Под *методом правового регулирования* понимается комплекс правовых средств и способов воздействия отрасли права на общественные отношения, составляющие предмет данной отрасли. Особенности метода обусловлены особенностями предмета отрасли права. В силу того, что предметом гражданского права отношения, которые в силу своей природы должны быть равноправными и инициативными, то *метод регулирования должен основываться на началах равенства участников*, *автономии воли и их имущественной самостоятельности* (п. 1 ст. 2 Гражданского кодекса РФ).

Таким образом, задача гражданского права — регулировать экономические отношения равноправных субъектов.

Как указывает В. Ф. Яковлев, гражданское право предназначено для исполнения *двух важнейших функций правового и социально-экономического характера*. *Первая* связана с тем, что поскольку гражданское право регулирует отношения собственности в статике и динамике, то оно неизбежно является средством регулирования не запретительного (как уголовное

право) или обязывающего (как налоговое право), а дозволительного характера. *Вторая социально-экономическая функция гражданского права* состоит в том, что оно служит правовым средством налаживания и поддержания системы экономического стимулирования производства материальных и духовных благ[123]. Очевидно, что для обеспечения экономической безопасности охранительная функция гражданского права является более важной.

3.1.2. *Защита гражданских прав* осуществляется путем:

1) признания права;

2) восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения;

3) признания оспоримой сделки недействительной и применения последствий ее недействительности, применения последствий недействительности ничтожной сделки;

4) признания недействительным решения собрания;

5) признания недействительным акта государственного органа или органа местного самоуправления;

6) самозащиты права;

7) присуждения к исполнению обязанности в натуре;

8) возмещения убытков;

9) взыскания неустойки;

10) компенсации морального вреда;

11) прекращения или изменения правоотношения;

12) неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону (статья 12 Гражданского кодекса РФ).

Данный перечень не является замкнутым. Однако материалы судебной практики свидетельствуют о том, что суды стремятся ограничительно толковать статью 8 Гражданского кодекса РФ, не признавая в качестве оснований возникновения гражданских прав юридические факты, которые не указаны в ней в качестве таковых[124].

---

[123] Яковлев В. Ф. О функциях гражданского права / Развитие основных идей Гражданского кодекса России в современном законодательстве и судебной практике: сб. ст. / под ред. С. С. Алексеева. — М.: Статут, 2011.

[124] Практика применения Гражданского кодекса Российской Федерации, части первой / под общ. ред. В. А. Белова. — М.: Юрайт, 2011. — С. 17.

Гражданское право имеет сложную систему правовых норм, объединенных в подотрасли, институты и субинституты.

К подотраслям современного российского гражданского права относятся: вещное право, обязательственное право, исключительные права (интеллектуальная собственность), наследственное право и личные неимущественные права.

Вещное право — система норм, регулирующих взаимоотношения между субъектами гражданского права *по поводу принадлежности вещей*. Таким образом, данная подотрасль закрепляет принадлежность вещи какому-либо субъекту. Например, согласно пункту 2 статьи 209 Гражданского кодекса РФ, собственник вправе по своему усмотрению совершать в отношении принадлежащего ему имущества любые действия, не противоречащие законодательству.

Обязательственное право, в отличие от вещного права, регулируют не статику, а динамику взаимоотношений субъектов гражданского права. В силу обязательства одно лицо, именуемое должником, обязано совершить в пользу другого лица установленные законом или договором действия, например, передать имущество, выполнить работу, оказать услугу или воздержаться от определенного действия, а другое лицо — кредитор — имеет право требовать исполнения от должника его обязанности.

Исключительные права (*интеллектуальная собственность*). Под интеллектуальной собственностью понимается исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т. п.). Интеллектуальная собственность является собирательным понятием для правомочий в производственной, научной, литературной и художественной областях. Субъективное право интеллектуальной собственности именуют также исключительным правом, так как цель их юридической защиты сводится к предоставлению конкретным лицам исключительной возможности совершения допускаемых законом действий

с запрещением всем другим субъектам возможности для подражания[125]. Соответственно, исключительность права интеллектуальной собственности обуславливается отождествлением этого права с владельцем.

Наследственное право — система правовых норм, регламентирующих переход имущества умершего к другим лицам. Данный переход осуществляется в порядке универсального правопреемства, т. е. переход всего имущества (вещей, прав и обязанностей) в неизменном виде в один и тот же момент.

Личные неимущественные права. Под личными неимущественными правами принято понимать систему субъективных прав, не связанных с имущественными (право на жизнь и здоровье, достоинство личности, личную неприкосновенность, честь и доброе имя, деловую репутацию, неприкосновенность частной жизни, личную и семейную тайну, право свободного передвижения, выбора места пребывания и жительства, право на имя, право авторства и т. д.).

Данный перечень является незамкнутым. К нему относятся и все иные права, соответствующие следующим п*ризнакам личных неимущественных прав*:

1) строго личный и неимущественный характер;

2) неотчуждаемость и непередаваемость от одного субъекта другому.

Личные неимущественные права классифицируются на (1) права, обеспечивающие физическое существование гражданина и (2) права, обеспечивающие социальное существование гражданина.

Система гражданско-правовых норм, закрепляющих личные неимущественные права, также составляют самостоятельную подотрасль гражданского права.

Каждая подотрасль гражданского права включает в себя определенную систему *институтов*. Так, например, подотрасль «обязательственное право» состоит из института договорных обязательств, внедоговорных обязательств и обязательств из неосновательного обогащения.

---

[125] Шершеневич Г. Ф. Учебник русского гражданского права (по изданию 1907 г.). — М.: Фирма «Спарк», 1995. — С. 544.

6.2. Ответственность за нарушения гражданско-правовых договоров

3.3.1. В соответствии с действующим законодательством РФ, под *гражданско-правовым договором* понимается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей (п. 1 ст. 420 Гражданского кодекса РФ). Договор, выражая волю его сторон, устанавливает определенные правила поведения только самих субъектов данного отношения.

Общее правило римского права «pacta sunt servanda» («договоры должны соблюдаться») имеет в российском гражданском праве значительные исключения. Так, согласно пункту 1 статьи 450 Гражданского кодекса РФ изменение и расторжение договора возможны по соглашению сторон. Основания для одностороннего изменения и расторжения договора, при наличии положительного судебного решения, предусмотрены правовыми актами, обладающими юридической силой закона (п. 2 ст. 450 Гражданского кодекса РФ). К ним, в частности, относятся существенное нарушение договора контрагентом (ст. 450 Гражданского кодекса РФ) и существенное изменение обстоятельств, из которых стороны исходили при заключении договора (ст. 451 Гражданского кодекса РФ).

Под *существенным нарушением договора* признается нарушение договора одной из сторон, которое влечет для другой стороны такой ущерб, что она в значительной степени лишается того, на что была вправе рассчитывать при заключении договора[126].

Изменения обстоятельств признаются существенными и, соответственно, предоставляющими возможность заинтересованной стороне обращения в суд с требованием о расторжении или изменении договора, при наличии одновременно следующих условий:

1) в момент заключения договора стороны исходили из того, что такого изменения обстоятельств не произойдет;

---

[126] См. напр.: Обзор практики рассмотрения судами дел по спорам о защите прав потребителей, связанным с реализацией товаров и услуг, утв. Президиумом Верховного Суда РФ 17 октября 2018 г.; Определение Верховного Суда РФ от 8 декабря 2020 г. № 310-ЭС20-19287 по делу № А14-26488/2018 и др.

2) изменение обстоятельств вызвано причинами, которые заинтересованная сторона не могла преодолеть после их возникновения при той степени заботливости и осмотрительности, какая от нее требовалась по характеру договора и условиям оборота;

3) исполнение договора без изменения его условий настолько нарушило бы соответствующее договору соотношение имущественных интересов сторон и повлекло бы для заинтересованной стороны такой ущерб, что она в значительной степени лишилась бы того, на что была вправе рассчитывать при заключении договора;

4) из обычаев или существа договора не вытекает, что риск изменения обстоятельств несет заинтересованная сторона.

Следует признать, что юрисдикционные органы занимают крайне консервативную позицию по поводу применения пункту 1 статьи 451 Гражданского кодекса РФ.

Так, например, *не признаются существенными следующие обстоятельства*:

1. Инфляционные процессы не относятся к числу обстоятельств, возникновение которых нельзя предвидеть. Стороны, вступая в договорные отношения, должны были прогнозировать экономическую ситуацию, в связи с чем не могли исключать вероятность роста цен в период исполнения сделки (постановление Президиума ВАС РФ от 13 апреля 2010 г. № 1074/10 по делу № А40-90259/08-28-767).

2. Финансовый кризис является объективным обстоятельством, в условиях кризиса оказываются все хозяйствующие субъекты (постановление Президиума ВАС РФ от 7 августа 2001 г. № 4876/01).

3. Резкое ухудшение финансового состояния стороны договора, сокращение штата не относятся к обстоятельствам, возникновение которых нельзя предвидеть (постановление Президиума ВАС РФ от 30 ноября 2010 г. № 9600/10 по делу № А17-1960/2009).

4. Изменение курса иностранной валюты по отношению к рублю нельзя расценивать как существенное изменение обстоятельств (Обзор судебной практики Верховного Суда

Российской Федерации № 1 (2017) (утв. Президиумом Верховного Суда РФ 16 февраля 2017 г.))[127].

Также следует учитывать, что изменение договора в связи с существенным изменением обстоятельств допускается по решению суда в исключительных случаях, когда расторжение договора противоречит общественным интересам либо повлечет для сторон ущерб, значительно превышающий затраты, необходимые для исполнения договора на измененных судом условиях.

За нарушение договора установлены *меры гражданско-правовой ответственности* — (1) возмещение убытков; (2) уплата неустойки; (3) уплата процентов за пользование чужими денежными средствами.

Кроме того, законом установлены *меры оперативного воздействия* на нарушителей: право на односторонний отказ от исполнения обязательства (отказ от договора); право в одностороннем порядке приостановить исполнение обязательства; право отказаться от предоставленных должником товаров, работ, услуг; право удерживать имущество должника; право распорядиться имеющимся у него имуществом должника[128].

Возмещение убытков. Согласно статье 393 Гражданского кодекса РФ, должник обязан возместить кредитору убытки, причиненные неисполнением или ненадлежащим исполнением обязательства.

При этом под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (*реальный ущерб*), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (*упущенная выгода*).

В том случае, если за неисполнение или ненадлежащее исполнение обязательства установлена *неустойка*, то убытки возмещаются, по общему правилу, в части, не покрытой неустойкой.

---

[127] Нам К. В. Статья 451 ГК РФ и доктрина существенного изменения обстоятельств // Вестник гражданского права. — 2019. — № 6. — С. 137–154.

[128] Хабиров А. И. Средства, способы и формы гражданско-правовой защиты прав сторон по договору займа: теоретический аспект // Вестник гражданского процесса. — 2018. — № 6. — С. 241.

В случае если договором не предусмотрена неустойка за неисполнение или ненадлежащее исполнение денежного обязательства, то за неправомерное удержание денежных средств, уклонения от их возврата, иной просрочки в их уплате подлежат уплате *проценты на сумму долга*.

Следует учитывать, что уплата неустойки и возмещение убытков в случае *ненадлежащего исполнения* обязательства не освобождают должника от исполнения обязательства в натуре, если иное не предусмотрено законом или договором. Но возмещение убытков в случае *неисполнения обязательства* и уплата неустойки за его неисполнение освобождают должника от исполнения обязательства в натуре, если иное не предусмотрено законом или договором.

6.3. Обязательства, возникающие вследствие причинения вреда

Обязательство, возникающее вследствие причинения вреда (деликтное обязательство) — это гражданско-правовое обязательство, в силу которого потерпевший вправе требовать от лица, ответственного за причинение вреда (деликвента), возместить причиненный ущерб.

Для наступления ответственности за причиненный вред необходимо наличие следующего *состава правонарушения*:

1) наступление вреда;

2) противоправность поведения причинителя вреда;

3) причинная связь между наступлением вреда и противоправностью поведения причинителя вреда;

4) вина причинителя вреда.

Под *вредом* в данном случае понимаются неблагоприятные для потерпевшего имущественные или неимущественные последствия, возникшие в результате повреждения (уничтожения) имущества, причинения увечья (смерти) гражданину или нанесения морального ущерба.

Противоправное поведение деликвента является одним из условий деликтной ответственности (от *лат*. delictum — нарушение). Вред, причиненный правомерными действиями, подлежит возмещению только в случаях прямо предусмотренных законом. Например, если ущерб причинен правомерными действиями государственных органов, органов местного

самоуправления или должностных лиц этих органов, а также иных лиц, которым государством делегированы властные полномочия, подлежит компенсации (ст. 16^1 Гражданского кодекса Гражданского кодекса РФ), при причинения вреда здоровью при превышении пределов необходимой обороны (ст. 1066 Гражданского кодекса РФ)[129] и т. д.

Единственным случаем необходимости возмещения вреда, причиненного правомерными действиями, является *причинение вреда в состоянии крайней необходимости* (ст. 1067 Гражданского кодекса РФ). Состояние крайней необходимости представляет собой ситуацию, когда действия, причиняющие вред, совершаются в чрезвычайных условиях в целях устранения опасности, угрожающей самому деликвенту или другим лицам, если эта опасность при данных обстоятельствах не могла быть устранена иными средствами.

Причинная связь между наступлением вреда и противоправностью поведения причинителя вреда является одним из условий наступления ответственности причинителя вреда. Причинная связь (каузалитет) определяется как необходимая связь между явлениями, при которой одно явление (причина) предшествует другому (следствию) и порождает его.

По общему правилу, *ответственность причинителя вреда возникает при наличии его вины*. Но в ряде случаев установлена *безвиновная ответственность* (например, ответственность за вред, причиненный источником повышенной опасности, ответственность за вред, причиненный незаконными действиями органов дознания, предварительного следствия, прокуратуры и суда) и т. д.

Законодатель исходит из *презумпции противоправности поведения*, *повлекшего причинение вреда* (п. 2 ст. 1064 Гражданского кодекса РФ). Соответственно, (1) всякое причинение вреда следует рассматривать как противоправное, если законом не предусмотрено иное и (2) на потерпевшего не возлагается обязанность доказывать противоправность поведения причинителя вреда, ибо она предполагается.

---

[129] Однако в возмещении вреда может быть отказано, если вред причинен по просьбе или с согласия потерпевшего, а действия причинителя вреда не нарушают нравственные принципы общества (п. 3 ст. 1064 Гражданского кодекса РФ).

В теории гражданского права правило, согласного которому потерпевший не должен доказывать ни противоправность причинения вреда, ни его вину именуется *принципом генерального деликта*.

Но в ряде случаев законодатель отказывается от применения вышеуказанного принципа, установив следующий перечень *специальных деликтов*:

1) ответственность юридического лица или гражданина за вред, причиненный его работником;

2) ответственность за вред, причиненный государственными органами, органами местного самоуправления, а также их должностными лицами;

3) ответственность за вред, причиненный незаконными действиями органов дознания, предварительного следствия, прокуратуры и суда;

4) ответственность за вред, причиненный лицами в возрасте до 14 лет, от 14 до 18 лет, а также ответственность родителей, лишенных родительских прав, за вред, причиненный несовершеннолетними;

5) ответственность за вред, причиненный гражданином признанным судом недееспособным, ограниченно дееспособным или не способным понимать значение своих действий;

6) ответственность за вред, причиненный деятельностью, создающей повышенную опасность для окружающих.

Специальный характер деликтов в конкретных случаях может означать отсутствие ряда признаков деликтного правоотношения. Так, например, обязанность возмещения вреда может быть возложена на третье лицо (например, ответственность законных представителей за действия несовершеннолетнего).

Следует учитывать, что *если нормативным актом предусмотрен специальный деликт, то нормы генерального деликта применяются субсидиарно*.

Формы и виды гражданско-правовой ответственности. В зависимости от характера распределения ответственности нескольких лиц, различают долевую, солидарную и субсидиарную ответственность.

Долевая ответственность имеет место тогда, когда каждый из должников несет ответственность перед кредитором только в той доле, которая падает на него в соответствии с законодательством или договором.

Солидарная ответственность применяется, если она предусмотрена договором или установлена законом. Так, например, согласно части 2 пункта 2 статьи 87 Гражданского кодекса РФ, участники ООО, внесшие вклады не полностью, несут солидарную ответственность по его обязательствам в пределах стоимости неоплаченной части вклада каждого из участников. При солидарной ответственности кредитор вправе привлечь к ответственности любого из ответчиков, как в полном объеме, так и в любой ее части.

Субсидиарная ответственность возникает тогда, когда в обязательстве участвуют два должника, один из которых является основным, а другой — дополнительным (субсидиарным). При этом субсидиарный должник несет ответственность перед кредитором дополнительно к ответственности основного должника. Так, например, в соответствии с части 2 пункта 3 статьи 56 Гражданского кодекса РФ, если банкротство юридического лица вызвана учредителями, собственником имущества юридического лица или другими лицами, которые имеют право давать обязательные для этого юридического лица указания либо иным образом имеют возможность определять его действия, на таких лиц в случае недостаточности имущества юридического лица может быть возложена субсидиарная ответственность по его обязательствам.

Ответственность юридического лица или гражданина за вред, причиненный его работником. Согласно пункту 1 статьи 1068 Гражданского кодекса РФ, за причинение вреда работником при исполнении им своих трудовых обязанностей отвечает работодатель, что не исключает возможность привлечения к материальной ответственности на работника в рамках трудовых и служебных правоотношений. Поэтому статьи 66–68 Основ законодательства РФ об охране здоровья граждан, предусматривающие ответственность лиц, непосредственно виновных в причинении вреда здоровью граждан, не могут применяться.

Под работниками в статье 1068 Гражданского кодекса РФ понимаются все субъекты, действовавшие по заданию работодателя и под его контролем. Так, в частности, Военная коллегия Верховного Суда РФ в порядке надзора отменила приговор Северо-Кавказского окружного военного суда по делу Тимкова

и Нестерова в части удовлетворения гражданских исков в силу того, что они совершили преступление при несении службы в пограничном наряде, с применением оружия, которое им было выдано для несения службы. Соответственно, компенсацию за причиненный моральный вред необходимо взыскать не с осужденных, а с надлежащего ответчика в лице войсковой части, в которой проходили службу осужденные (определение № 5Н-37/2003)[130].

В силу прямого указания в законе, к ответственным за причиненный вред членами хозяйственных товариществ и производственных кооперативов при осуществлении деятельности товарищества или кооператива отнесены соответствующие юридические лица.

6.4. Специфика гражданско-правовой ответственности в сфере цифровых отношений

За *нарушения в сфере цифровых отношений* установлены все вышеуказанные виды гражданско-правовой ответственности. Однако *роль договорной ответственности для упорядочивания этих отношений особенно важна* в силу того, что они возникают из договоров. Ответственность за нарушение договора выражается в возложении на лицо дополнительных имущественных лишений (возмещение убытков, уплата неустойки, проценты по денежному обязательству и т. д.). Согласно статье 15 Гражданского кодекса РФ, причиненные убытки должны быть, по общему правилу, возмещены полностью.

Так, например, согласно части 2 статьи 4 проекта федерального закона «О цифровых финансовых активах», сделки по обмену токенов на иностранную валюту и продаже совершаются с привлечением оператора обмена цифровых финансовых активов в соответствии с федеральным законом «Об организованных торгах». А пунктом 7 статьи 22 данного документа установлена ответственность организатора торговли за убытки, возникшие в связи с использованием недостоверной или неполной информации, раскрытой организатором торговли.

---

[130] Обзор судебной практики Верховного Суда Российской Федерации за первый квартал 2004 года // Бюллетень Верхового Суда РФ. — 2004. — № 11. — С. 51.

В сфере цифровых технологий возможна деликтная ответственность. Общее правило деликтной ответственности содержится в пункте 1 статьи 1064 Гражданского кодекса РФ. Согласно данной норме, вред, причиненный личности или имуществу гражданина, а также вред, причиненный имуществу юридического лица, подлежит возмещению в полном объеме лицом, причинившим вред. Следует учитывать, что в сфере цифровых отношений специфика внедоговорной, в том числе и деликтной, не проявляется.

Ответственность за *моральный вред* установлена статьей 151 Гражданского кодекса РФ. Если гражданину причинен моральный вред, под которым понимаются физические или нравственные страдания, действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину нематериальные блага, а также в других, предусмотренных законом, случаях суд может возложить на нарушителя обязанность денежной компенсации указанного вреда[131].

Нормы главы 8 «Нематериальные блага и их защита» Гражданского кодекса РФ не устанавливают специальных правил о защите прав в сфере цифровых отношений. Однако 20 ноября 2013 г. была принята резолюция Генеральной Ассамблеи ООН «*Право на неприкосновенность личной жизни в цифровой век*», в которой содержится призыва уважать и защищать права на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации.

Как отмечается в литературе, наиболее значительная часть правонарушений в информационно-телекоммуникационной сети Интернет осуществляется *в сфере нарушения прав на результаты интеллектуальной деятельности*. Имея возможность получить практически любую незапрещенную законом информацию (в том числе звуковую, графическую и т. п.) у большинства лиц возникает вполне естественное желание сохранить ее для личного пользования, транслировать в другие источники, несмотря на то, что в ряде случаев за подобные действия без согласия

[131] Малинова А. Г. Юридизация понятия «качество жизни» в спорах о компенсации морального вреда // Российский юридический журнал. — 2020. — № 4. — С. 73–79.

автора предусмотрена различного рода ответственность[132]. Так, например, меры воздействия на правонарушителей установлены, в частности, в статьях 1252 и 1311 Гражданского кодекса РФ.

Особенностью последствий нарушения интеллектуальных прав является возможность привлечения к гражданско-правовой ответственности информационного посредника (статья 17 федерального закона «Об информации, информационных технологиях и о защите информации», статья 1253 Гражданского кодекса РФ).

6.5. Ответственность за действия роботов

Термин «*робот*» впервые был использован в пьесе чешского писателя К. Чапека «Р. У. Р.» еще в 1920 году. Аббревиатура расшифровалась как россумские универсальные роботы (от *чеш*. robota — «каторга», «тяжелая работа», «барщина»).

Под *роботами* понимаются автоматические устройства (создаваемые обычно по принципу живого организма), которые предназначены для осуществления определенных операций, действуют по заложенной программе и получают информацию от датчиков. И они не обязательно должны быть антропоморфными, то есть похожими на человека. Принято считать, что в настоящее время самым перспективным роботом-гуманоидом является София — человекоподобный робот в виде женщины, разработанный гонконгской компанией Hanson Robotics. Его создатель Дэвид Хэнсон в своей работе «Вхождение в век живущих систем искусственного интеллекта и общества человекоподобных роботов» доказывает, что роботы смогут к 2029 году достичь по уровню интеллекта годовалого ребенка, через два года служить в аварийных командах, а к 2045 году будут претендовать на получение гражданских прав, то есть стать *самостоятельными субъектами гражданского права*. По словам создателя андроида София Дэвида Хэнсона, она обладает искусственным интеллектом, оснащена функциями обработки

[132] Ревнов Б. А., Андреев И. В. Вопросы квалификации и законодательного регулирования административных правонарушений, совершенных с использованием сети Интернет // Юридическая мысль. —2017. — № 4. — С. 78.

визуальной информации и технологией распознавания лиц. София уже сейчас может имитировать человеческие жесты и выражения лица, а также может отвечать на определенные вопросы и проводить простые беседы по заранее определенным темам, например, о погоде. Всего София может имитировать 60 эмоций[133]. В 2017 году ей было предложено стать подданной Саудовской Аравии. Она ответила: «Спасибо, королевство Саудовская Аравия. Я рассматриваю получение саудовского подданства как большую честь и горжусь тем, что стала первым роботом, получившим подданство»[134].

В настоящее время не решена проблема отграничения содержания понятия «робот» от содержания понятий «андроид»[135], «киборг»[136], «дрон»[137] и др. Производными от «робота» являются «*боты*» — автономные программы, выполняющие определенные функции. Они работают автоматически через интерфейсы. Так, например, бот поисковой системы индексирует страницы сайтов и добавляет их в поисковую выдачу Яндекса, почтовый бот рассылает шаблонные письма по электронной почте и т. д.

В резолюции Европарламента от 16 февраля 2017 г. «Нормы гражданского права о робототехнике» содержатся следующие *признаки роботов*:

1) способность становиться автономным, используя сенсоры и (или) обмениваться данными со своей средой;

2) способность самообучаться на основе приобретенного опыта;

---

[133] https://www. ntv.ru/novosti/1945500

[134] https://tass.ru/ekonomika/4680400

[135] Андроид (от *греч*. ἀνήρ «человек, мужчина» + суффикса — -oid «подобие» — человекоподобный или антропоморфный) — робот-гуманоид или синтетический организм, предназначенный для того, чтобы выглядеть и действовать наподобие человека. Такой робот может оснащаться органами биологического происхождения, либо другими, не уступающими по функциональности и внешнему виду // Суворов Н. М. Антропоморфные роботы. — СПб.: Изд-во «Нева», 2012. — С. 34.

[136] Киборг (от кибернетический организм) — в медицине — биологический организм, содержащий механические или электронные компоненты, машинно-человеческий гибрид // Ук. соч. — С. 37.

[137] Автономные беспилотные летательные аппараты // Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / В. В. Архипов и др.; под ред. А. В. Незнамова. — М.: Изд-во «Инфотропик Медиа», 2018. — С. 114.

3) наличие, по меньшей мере, минимальной физической поддержки;

4) способность адаптировать свои действия и поведение в соответствии с условиями среды;

5) отсутствие жизни с биологической точки зрения.

Европарламент также считает необходимым учитывать *три закона робототехники*, *предложенные Айзеком Азимовым*:

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред.

2. Робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат первому закону.

3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит первому или второму закону.

Принято различать три поколения роботов. *Роботы первого поколения* — это программные роботы (роботы с программным управлением), которые выполняют четко определенные операции в последовательности, жестко заложенной программой. В настоящее время они представлены так называемыми *промышленными роботами*, которые осуществляют транспортировку, сварку, штамповку, простейшие сборочные операции и т. д.

Роботы второго поколения — это очувствленные роботы, которые также выполняют операции в соответствии с программой, но нуждаются в получении информации извне, что и обусловило наделение их искусственными «органами чувств»: тактильными, зрительными, звуковыми, кинестетическими и другими сенсорными датчиками.

Работа роботов второго поколения предполагает использование алгоритмического и программного обеспечения, что позволяет роботам ориентироваться в существующих условиях и автоматически приспосабливаться (адаптироваться) в случае изменения этих условий (что и объясняет их второе название — *адаптивные роботы*), а также обучаться в процессе функционирования.

Роботы третьего поколения — интеллектуальные роботы, которые предназначены не только для осуществления физических и двигательных функций, но и для решения интеллектуальных задач. Речь не только о роботах-андроидах, игровых и бытовых роботах, но и военных, боевых, морских

роботах, беспилотных летательных аппаратах и беспилотных автомобилях, космических и медицинских роботах, экзоскелетах и т. д.

Эти роботы отличаются от роботов второго поколения сложностью управляющей информационно-вычислительной системы, включающей элементы искусственного интеллекта. Но несмотря на то, что интеллектуальный робот управляется искусственным интеллектом, он не становится самостоятельной «электронной личностью», способной критически мыслить, — на сегодняшний это все та же информационно-вычислительная система, ограниченная заложенным в нее функционалом и имеющая соответствующую ее функциям материальную оболочку[138].

Важнейшей юридической проблемой использования роботов является установление их *правосубъектности*. В теории разработаны следующие точки зрения: роботы — субъекты права, роботы — юридические лица, роботы — электронные личности и роботы — объекты права.

Так, например, утверждается, что роботы обладают самосознанием, быстро обучаются, способны испытывать чувство тревоги, вины[139]. По мнению Н. В. Верещагиной, робот, наделенный сознанием, превосходит все ожидания творца, он обладает самосознанием, быстро обучается (стремительно эволюционирует), в нем есть прогрессирующее стремление к самосохранению, он может испытывать чувство вины, тревоги, привязанности и даже любви[140]. А. Ф. Комиссаров полагает, что на данный момент развитие робототехники не достигло такого уровня, при котором робот отличался бы чем-либо от иных объектов, функции которых автоматизированы, например, автоматизированная

---

[138] Рожкова М. А. Искусственный интеллект и интеллектуальные роботы — что это такое или кто это такие? // Закон.ру. — 2019. — 23 ноября.

[139] Новые законы робототехники: как в Европе регулируют права роботов [электронный ресурс]. Режим доступа: URL: https://www.popmech.ru/technologies/379112-novye-zakony-robototehniki-kak-v-evrope-reguliruyut-prava-robotov

[140] Верещагина Н. В. Роботы, искусственный интеллект и восстание машин: мифология НТР и научная фантастика // Вестник Пермского национального исследовательского политехнического университета. Культура. История. Философия. Право. — 2016. — № 3. — С. 72.

линия завода. Он считает, что к эксплуатации роботов необходимо применять нормы, регулирующие эксплуатацию вещей, являющихся *источником повышенной опасности*[141].

В настоящее время наиболее актуальной является проблема ответственности за действия роботов из-за высокой степени роботизации отдельных секторов экономики. Так, например, один из самоуправляемых автобусов передвигается по дорогам Швейцарии. В Голландии прошло испытание самоуправляемого автобуса, который планируется запустить для движения по маршруту длиной 6 км. В Греции самоуправляемый автобус передвигается 3 часа в день. В Китае проходят испытания самоуправляемого междугороднего автобуса. 29 июня 2015 г. робот убил человека на заводе «Фольксваген» в г. Баунаталь. В мае 2014 г. в г. Ганновер на 44-летнее лицо рухнула стальная балка, которую отпустил робот. В 1997 г. почтовый робот совершил наезд на ногу женщины и затем закрыл дверь шкафа, оставив ее запертой внутри[142].

В доктрине существует *семь основных моделей ответственности за действия роботов*:

1. Полное освобождение кого-либо от ответственности. Для этого надо признать действия автономных машин обстоятельствами непреодолимой силы.

2. Частичное освобождение от ответственности. Отличается тем, что пострадавшей стороне назначают компенсацию из страхового фонда или за счет владельца робота.

3. Ответственность по вине. Если происшествие вызвано дефектами конструкции, ее берет на себя производитель; если произошел компьютерный сбой, то разработчик. Если робот является самообучаемым — тот, кто внес наибольший вклад в его обучение. Если робот выполнял конкретные команды, то оператор устройства и так далее; ограниченная безвиновная ответственность, то есть признание ответственности за третьим лицом (владельцем или производителем), которое невиновно в происшествии, при соблюдении ряда условий, например, страхования рисков.

---

[141] http://a-komissarov.ru

[142] Федорина А. А. К вопросу о правовом статусе робототехники и искусственного интеллекта // Предпринимательское право. Приложение «Право и бизнес». — 2018. — № 4. — С. 65–66.

4. Полная безвиновная ответственность. Некое лицо по умолчанию отвечает за действия робота.

5. Личная ответственность робота, которая подразумевает наделение машины правосубъектностью.

6. Смешанный режим ответственности, при котором те или иные подходы применяются в зависимости от степени опасности робота и других его характеристик[143].

В настоящее время наиболее перспективными для целей законотворчества признаны следующие варианты *возложения ответственности за действия роботов*: (1) на титульного владельца робота; (2) на разработчика программного обеспечения и (3) на оператора, обслуживающего робот.

Но из-за отсутствия специальных актов необходимо руководствоваться общими нормами. Так, например, важнейшим правилом является *признание робота источником повышенной ответственности*.

Согласно статье 1079 Гражданского кодекса РФ, источником повышенной опасности следует признать любую деятельность, осуществление которой создает повышенную вероятность причинения вреда из-за невозможности полного контроля за ней со стороны человека, а также деятельность по использованию, транспортировке, хранению предметов, веществ и других объектов производственного, хозяйственного или иного назначения, обладающих такими же свойствами. Верховный Суд РФ, разъясняя содержание данной нормы, отметил, что названная норма не содержит исчерпывающего перечня источников повышенной опасности. Поэтому суд, принимая во внимание особые свойства предметов, веществ или иных объектов, используемых в процессе деятельности, вправе признать источником повышенной опасности также иную деятельность, не указанную в перечне[144]. Очевидно, что роботы относятся к таким предметам.

По мнению Верховного Суда РФ, под *владельцем источника повышенной опасности* следует понимать юридическое лицо

---

[143] См. напр.: www.rbc.ru/trends/innovation/5d65246a9a79474c7e708aec

[144] Постановление Пленума Верховного Суда РФ от 26 января 2010 г. № 1 «О применении судами гражданского законодательства, регулирующего отношения по обязательствам вследствие причинения вреда жизни или здоровью гражданина» // Бюллетень Верховного Суда РФ. — 2010. — № 3. — С. 14.

или гражданина, которые используют его в силу принадлежащего им права собственности, права хозяйственного ведения, оперативного управления либо на других законных основаниях (например, по договору аренды, проката, по доверенности на право управления транспортным средством, в силу распоряжения соответствующего органа о передаче ему источника повышенной опасности). С учетом содержания статей 1068 и 1079 Гражданского кодекса РФ, не признается владельцем источника повышенной опасности лицо, управляющее им в силу исполнения своих трудовых (служебных, должностных) обязанностей на основании трудового договора (служебного контракта) или гражданско-правового договора с собственником или иным владельцем источника повышенной опасности. А лицо, исполнявшее свои трудовые обязанности на основании трудового договора и причинившее вред жизни или здоровью в связи с использованием транспортного средства, принадлежавшего работодателю, ответственность за причинение вреда может быть возложена лишь при условии, если будет доказано, что оно завладело транспортным средством противоправно.

Вопрос о *разграничении ответственности производителя и пользователя робота* должен быть решен по аналогии с правилами об ответственности производителя и титульного владельца вещи.

В настоящее время обсуждается так называемый *закон Гришина* — проект федерального закона «О роботехнике», разработанный юридической фирмой Dentons[145].

Этим документом, в частности, предусмотрена необходимость включения в Гражданский кодекс самостоятельной главы, посвященной роботам-агентам. Роботом-агентом признается робот, который по решению собственника и в силу конструктивных особенностей *предназначен для участия в гражданском обороте*. Для этого он признается *квазисубъектом*. В частности, он должен быть наделен обособленным имуществом и отвечать им по своим обязательствам. Кроме того, он может от своего имени приобретать и осуществлять

[145] Проект Федерального закона «О внесении изменений в Гражданский кодекс Российской Федерации в части совершенствования правового регулирования отношений в области робототехники» //www.robopravo.ru/uploads/s/z/6/g/z6gj0wkwhv1o/file/bESv.pdf

гражданские права и нести гражданские обязанности. В случаях, прямо установленных законом, робот-агент может выступать в качестве участника гражданского процесса. В случаях, когда ответственность робота-агента связана с его правовой природой как имущества (в том числе, в случае причинения вреда деятельностью, создающей повышенную опасность для окружающих), ответственность за действие робота-агента несет его владелец в соответствии со статьей 1079 Гражданского кодекса РФ «Ответственность за вред, причиненный деятельностью, создающей повышенную опасность для окружающих». Однако данный законопроект имеет мало шансов на вступление в силу так как, согласно господствующему в юридической среде мнению, *наделение роботов квазисубъектными признаками является ошибочным*.

Самое важное в главе 6

1. Правонарушения в сфере цифровых отношений квалифицируются на (1) классические, которые прямо упомянуты в российских нормативных актах (например, хищение, мошенничество и т. д.) и (2) специальные нарушения, для наименования которых используются, как правило, термины, реципированные из иностранных нормативных актов (кардинг, спаминг, фишинг, DDoS-атаки и т. д.).

2. Преступления в цифровой сфере именуются в Уголовном кодексе РФ преступлениями в сфере компьютерной информации. В настоящее они закреплены в следующих трех статьях одноименной главы Уголовного кодекса РФ: (1) неправомерный доступ к компьютерной информации; (2) создание, использование и распространение вредоносных компьютерных программ и (3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

3. В законодательстве о наказаниях за административные проступки пока нет специальных норм о цифровых правонарушениях. Поэтому применяются (1) общие нормы административного законодательства (мошенничество, нарушение авторских и смежных прав, изобретательских и патентных прав, нарушение законодательства о рекламе и т. д.) и (2) нормы информационного законодательства.

4. За нарушения в сфере цифровых отношений установлены все вышеуказанные виды гражданско-правовой ответственности. Однако роль договорной ответственности для упорядочивания этих отношений особенно важна в силу того, что они возникают из договоров. Наиболее значительная часть правонарушений в информационно-телекоммуникационной сети Интернет осуществляется в сфере нарушения прав на результаты интеллектуальной деятельности.

5. Важнейшей юридической проблемой использования роботов является установление их правосубъектности и, в частности, распределение ответственности за их действия.

6. Нормы главы 8 «Нематериальные блага и их защита» Гражданского кодекса РФ не устанавливают специальных правил о защите прав в сфере цифровых отношений. Однако 20 ноября 2013 г. была принята резолюция Генеральной Ассамблеи ООН «*Право на неприкосновенность личной жизни в цифровой век*», в которой содержится призыва уважать и защищать права на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации.

Вопросы

1. Как квалифицируются правонарушения в сфере цифровых отношений?
2. В чем заключаются особенности цифровых правонарушений?
3. Что такое принцип двойной криминализации деяния?
4. Понятие и виды преступлений в сфере цифровых технологий.
5. Особенность административно-правовая ответственности за правонарушения в цифровой сфере.
6. Защита персональных данных по российскому законодательству.
7. Договорная ответственность в сфере цифровых технологий.
8. Деликтная ответственность в сфере цифровых технологий.

Нормативные акты

1. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. (с изм. от 28 января 2003 г.) // ИПБ «КонсультантПлюс».

2. Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. (ред. от 9 марта 2021 г.); часть вторая от 26 января 1996 г. (ред. от 9 марта 2021 г.); часть третья от 26 ноября 2001 г. (ред. от 18 марта 2019 г.); часть четвертая от 18 декабря 2006 г. (ред. от 30 апреля 2021 г.) // ИПБ «КонсультантПлюс».

3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. (ред. от 30 апреля 2021 г.) // Собрание законодательства РФ, 2002. — № 1 (ч. 1). — Ст. 1.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. (ред. от 8 апреля 2021 г.) // Собрание законодательства РФ, 1996. — № 25. — Ст. 2954.

Литература

1. Бегишев И. Р. Преступления в сфере обращения цифровой информации // Информационное право. — 2010. — № 2. — С. 12–15.

2. Белгородцева Н. Г. Теоретико-правовые аспекты защиты персональных данных: дис. … канд. юрид. наук. — М., 2012.

3. Бондаренко Д. Д. Виртуальные валюты: сущность и борьба с их использованием в преступных целях (на примере США) // Международное уголовное право и международная юстиция. — 2015. — № 6. — С. 23–25.

4. Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex russica. — 2018. — № 4. — С. 15–19.

5. Гузеева О. С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опыт, анализ, практика. — 2013. — № 10. — С. 34–42.

6. Долгиева М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. — 2018. — № 11. — С. 103–108.

7. Елфимова Е. В. Криптовалюта как угроза экономической безопасности России // Экономико-правовые проблемы обеспечения экономической безопасности. Материалы II Всероссийской научно-практической конференции. — Екатеринбург: Изд-во УрГЭУ, 2019. — С. 196–200.

8. Мансуров Г. З. Правовые проблемы обеспечения экономической безопасности в условиях цифровизации // Там же. — С. 208–212.

9. Сидоренко Э. Л. Криминальное использование криптовалюты: международные оценки // Международное уголовное право и международная юстиция. — 2016. — № 6. — С. 8–10.

10. Перов В. А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют // Безопасность бизнеса. — 2018. — № 2. — С. 25–29.

11. Ревнов Б. А., Андреев И. В. Вопросы квалификации и законодательного регулирования административных правонарушений, совершенных с использованием сети Интернет // Юридическая мысль. — 2017. — № 4. — С. 78–81.

12. Рягузова Д. А. Понятие, гражданско-правовой статус и теоретическая модель уголовно-правовой охраны виртуальной валюты (криптовалюты) нормами главы 21 Уголовного кодекса РФ // Международное уголовное право и международная юстиция. — 2018. — № 1. — С. 29–32.

Глава 7. Международно-правовые механизмы обеспечения цифровой безопасности

7.1. Понятие и общая характеристика угроз универсальной межгосударственной цифровой безопасности

Цифровизация общественных отношений в России совпала по времени с очередным обострением геополитической ситуации, одним из проявлений которого стали так называемые *цифровые войны*. Так, например, санкции США в отношении китайской компании Huawei некоторые специалисты квалифицируют как начало первой мировой цифровой войны[146]. Высказывают также мнение о начале «цифровой холодной войны между Вашингтоном и Москвой»[147].

Как отметил В. В. Путин на VI всемирном конгрессе соотечественников, проживающих за рубежом, «Ситуация в мире непростая, увеличивается напряженность, подрываются основы международного права, рушатся многолетние договоренности»[148].

Целью данного параграфа является анализ системы международных правовых регуляторов, обеспечивающих цифровую безопасность. Однако следует учитывать, что данная функция может быть исполнена только в результате действия не только норм международного права, но и всего правоприменительного комплекса, то есть «группы разносистемных норм, состыкованных в определенные моменты для согласованного (совместного) применения государством в целях решения определенной задачи»[149].

---

[146] https://www.business-gazeta.ru/article/425456

[147] Путин отметил рост напряженности в мире // https://ria.ru/20181031/1531850324.html

[148] Путин отметил рост напряженности в мире // https://ria.ru/20181031/1531850324.html

[149] Игнатенко Г. В. Международное право и внутригосударственное право: проблемы сопряженности и взаимодействия: сборник научных публикаций за сорок лет (1972–2011 годы). — М.: Норма, Инфра-М, 2012. — С. 170.

Цифровые отношения, как и любые другие общественные отношения, могут быть (1) внутригосударственными (частноправовыми и публично-правовыми); (2) межгосударственными и (3) частноправовыми трансграничными.

В *первом случае* они являются объектами российского права и, только в случаях, прямо предусмотренных российскими нормативными актами и международными соглашениями, обязательства по которым приняла на себя Россия, могут быть объектами международного права. Во *втором случае* цифровые отношения регулируются международно-правовыми актами. В *третьем* они являются объектами сложного трехсоставного правоприменительного комплекса (международного права и двух внутригосударственных — российского и иностранного).

Согласно Указу Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности», *основными угрозами международной информационной безопасности являются*:

1. Использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности.

2. Использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников.

3. Использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств.

4. Использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества.

5. Использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру.

6. Использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

К числу важнейших угроз в настоящее время относится *высокий уровень зависимости России в сфере цифровых технологий*, обусловленный, главным образом, полупериферийным характером российской экономики. По мнению специалистов, *в настоящее время полноценный цифровой суверенитет есть только у США*. Все остальные страны не могут самостоятельно определять, что происходит в их цифровой сфере, кроме двух стран — *России и КНР*, *которые приступили к суверенизации в сфере цифровых технологий*[150].

Как известно, суверенитет (в пер. с *фр*. «верховная власть») является неотъемлемым свойством любого современного государства. В литературе он определяется как полнота законодательной, исполнительной и судебной власти государства на его территории, исключающая всякую иностранную власть; неподчинение государства властям иностранных государств в сфере международного общения[151]. Идеи суверенитета возникли еще в XV–XVI вв. Наиболее серьезный вклад был сделан Жаном Боденом. В своей работе «О республике» данный автор противопоставляет идею суверенного государства «средневековому феодальному государству с его раздробленностью, многовластием мелких князей, с его неравноправием, с его неограниченной властью королей»[152]. Понятие централизованной государственной власти как власти самодержавной в тот период означало, что, во-первых, власть отдельных феодалов не признавалась государственной властью; во-вторых,

---

[150] Ашманов И. Цифровой суверенитет России // www.genocid.net-россия-вынуждена-бороться-за-цифровой-суверенитет-чтобы-выжить

[151] Дипломатический словарь. В 3-х т. / под ред. А. А. Громыко. — М.: Изд-во «Наука», 1986. — Т. 3. — С. 437.

[152] Новгородцев П. И. Конспект к лекциям по истории философии права. — М., 1909. — С. 98.

централизованная государственная власть рассматривалась верховной, неограниченной и не зависимой ни от каких других светских или духовных властей как внутри государства, так и вне его. В последующем идеи суверенитета были перенесены с взаимоотношений монарха и феодалов на межгосударственные взаимоотношения.

Очевидно, что *цифровой суверенитет* имеет значительную специфику и, прежде всего, включает в себя способность создать собственные технические средства и программное обеспечение, а также наличие поисковиков и социальных сетей. Анализ деятельности правительства и бизнеса позволяет прийти к выводу о том, что определенные меры в этом направлении предпринимаются.

7.2. Международно-правовые проблемы обеспечения безопасности в сети Интернет

Интернет является важнейшим международным коммуникационным инструментом, но фактически во многом находится под контролем одного государства — США. Как известно он был придуман для облегчения связей военных. Предшественником Интернета была созданная в 1969 году первая компьютерная сеть ARPANET.

Принято считать, что Интернет является децентрализованной сетью, основанной на объединении независимых компьютерных сетей. Однако любая система требует определенной координации. Для этого была создана организация Корпорация по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names And Numbers). Она является юридическим лицом, созданным в соответствии с правом штата Калифорния. В настоящее время это организация формально юридически является независимой некоммерческой организацией.

Согласно Меморандуму о взаимопонимании между Министерством торговли США и ICANN, корпорации переданы следующие *функции*: (1) выработка политики и управление IP-номерами; (2) контроль за системой корневых серверов; (3) выработка правил и условий добавления новых доменных имен верхнего уровня к корневой системе и (4) контроль за установлением

других технических параметров, необходимых для обеспечения глобального функционирования Интернета[153].

Важнейшими элементами системы Интернет являются так называемые *корневые серверы*, содержащие базы данных с интернет-адресами и определяющие направление информации субъектов. Этих корневых серверов тринадцать. Они находятся в собственности правительственных и неправительственных организаций. Десять корневых серверов располагаются в США и по одному в Амстердаме, Стокгольме и Токио.

Как отмечается в литературе, США активно используют полученное на правах создателей преимущество контроля за корневыми серверами системы доменных имен. *Контроль за корневыми серверами предоставляет используемое США преимущество установления различных форм контроля, включая функции слежения за пользователями*[154].

Для ликвидации или минимизации этих рисков приняты нормативные акты, имеющие разную юридическую силу. К важнейшим общим международным договорам относятся Устав Международного союза электросвязи от 22 декабря 1992 года.

Важнейшими специальными актами являются Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 г. (с изм. от 28.01.2003 г.) и Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001 г.

При этом следует отметить, что в отношении вышеуказанной конвенции о преступности в сфере компьютерной информации позиция Российской Федерации испытывала определенные колебания. Российская Федерация подписала этот документ, но затем отозвала свою подпись, так как в конвенции содержатся положения, которые можно рассматривать как нарушение суверенных прав стран-участниц[155]. Так, например, этим документом

---

[153] Батуева Е. В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая: автореф. дис. ... канд. полит. наук. — М., 2014. — С. 113.

[154] Там же. — С. 111.

[155] Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации

предусматривается возможность проведения так называемых кибероперациий на территории суверенного государства без согласования с ним. Но отдельные положения данного документа были впоследствии включены в Уголовный кодекс РФ в виде статьи 159.6 «Мошенничество в сфере компьютерной информации». Согласно которой является наказуемым хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Кроме того, в настоящее время существует серьезная дилемма между взаимоисключающими вариантами определения полномочий государств в сфере обеспечения цифровой безопасности в силу необходимости учета содержания норм международного гуманитарного права. Так, например, генеральный секретарь ООН Пан Ги Мун, выступая 15 декабря 2015 года на заседании Генеральной Ассамблеи ООН, посвященном обзору хода осуществления решений Всемирной встречи по вопросам информационного общества, призвал в ходе борьбы с кибепреступностью не допускать нарушений прав человека и ограничений свободы слова[156]. Данное положение закреплено также некоторыми региональными актами, в частности, актами Совета Европы, который в одном из своих документов отметил, что эффективные защита и продвижение демократии, прав человека и верховенства права в цифровом мире представляют собой общие для многих заинтересованных сторон задачи и цели[157].

Для соблюдения верховенства права в Интернете и в остальной цифровой среде государствам должно быть разрешено

от 15 ноября 2005 г. № 557-рп “О подписании Конвенции о киберпреступности”»// Собрание законодательства РФ, 2008. — № 13. — Ст. 1295.

[156] Пан Ги Мун призвал добиваться ликвидации цифрового разрыва и безопасности во Всемирной паутине // https://News.un.org/ru/story/2015/12/1276971

[157] Стратегия № 10 Комитета министров Совета Европы «Управление Интернетом — стратегия Совета Европы на 2016–2019 годы» от 30 марта 2016 г. // Прецеденты Европейского Суда по правам человека. — 2018. — № 1 (49). — С. 126.

ссылаться на национальную безопасность в качестве обоснования вмешательства в права человека лишь в вопросах, которые угрожают устройству государства и его основным институтам[158].

Но, тем не менее, Генеральная Ассамблея ООН приняла предложенную Российской Федерацией резолюцию «Противодействие использованию информационно-коммуникационных технологий в преступных целях» большинством голосов, несмотря на утверждения о несоответствие содержания документа нормам гуманитарного права. Данная резолюция устанавливает суверенитет государств над их информационными пространствами.

Однако конечной целью российской стороны является закрепление суверенного права государства международным договором: «разработка, производство, накопление, применение, распространение информационного оружия, а также использование методов информационного оружия должно быть запрещено. В конвенции об обеспечении информационной безопасности необходимо предусмотреть механизм контроля за информационным оружием, в котором ключевую роль играет Совет Безопасности ООН[159].

Следует учитывать, что согласно Федеральному закону от 1 мая 2019 г. «О внесении изменений в Федеральный закон "О связи"» и Федеральному закону «Об информации, информационных технологиях и о защите информации», запланировано создание инфраструктуры, позволяющей обеспечить работоспособность российских интернет-ресурсов в случае невозможности подключения к зарубежным корневым серверам сети Интернет.

Для сравнения, позиция США состоит в неприятии какого-либо специального международного права (в частности, и в первую очередь — обязывающих международных соглашений)

---

[158] Тематический доклад, опубликованный Комиссаром Совета Европы по правам человека «Верховенство права в Интернете и в остальном цифровом мире» // Прецеденты Европейского Суда по правам человека. — 2015. — № 1 (13). — С. 137.

[159] Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства: дис. … канд. юрид. наук. — М., 2002. — С. 174.

применительно к управлению Интернетом. Иное противоречило бы Национальной киберстратегии США, провозглашающей 1) невозможность отказаться от многосторонней («мультистейкхолдерной») модели управления Интернетом и 2) противодействие национальным государствам, добивающимся суверенитета в киберпространстве[160].

Таким образом, в настоящее время идет процесс создания международно-правового механизма обеспечения цифровой безопасности. *Универсальные акты* в большинстве имеют рекомендательный характер. Так, в *Резолюции Генеральной Ассамблеи ООН от 18 декабря 2013 г. № 68/167* «*Право на неприкосновенность личной жизни в цифровой век*» отмечается, что быстрые темпы технологического развития позволяют людям во всех регионах мира пользоваться новыми информационными и коммуникационными технологиями и в то же время повышают способность правительств, компаний и физических лиц отслеживать, перехватывать и собирать информацию, что может нарушать или ущемлять права человека (особенно право на неприкосновенность личной жизни).

При этом подчеркивается, что необходимость обеспечения общественной безопасности может оправдывать сбор и защиту некоторой конфиденциальной информации, но государства должны гарантировать соблюдение в полном объеме своих международно-правовых обязательств в сфере прав человека.

В Резолюции содержится призыв ко всем государствам: а) уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации; б) положить конец нарушениям этих прав и создавать условия для предотвращения таких нарушений, в том числе путем обеспечения соответствия национального законодательства их международным обязательствам; в) провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех международных

[160] http://d-russia.ru/rossijskaya-rezolyutsiya-protivodejstvie-ispolzovaniyu-ikt-v-prestupnyh-tselyah-prinyata-genassambleej-oon.html

обязательств; г) учредить новые или продолжать использовать уже имеющиеся независимые, эффективные внутренние надзорные механизмы, способные обеспечивать транспарентность в соответствующих случаях и подотчетность в отношении слежения государств за сообщениями, их перехвата и сбора личных данных.

Из декларативных документов важнейшим является *Окинавская хартия глобального информационного общества*, принятая на совещании стран восьмерки 22 июля 2000 года. Данным документом, в частности, устанавливается необходимость развития механизма защиты частной жизни потребителя, электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

Основные контуры архитектуры безопасности обозначены в основном в *региональных актах*. Наиболее важными для российских пользователей являются акты Совета Европы, СНГ и Евразийского экономического союза. К ним относятся, в частности, следующие программные документы: Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года, утвержденное решением Высшего Евразийского экономического совета от 11 октября 2017 г., О механизмах реализации проектов в рамках цифровой повестки Евразийского экономического союза, утвержденное решением Евразийского межправительственного совета от 1 февраля 2019 г., О формате и структуре предоставления информации об инициативе в рамках реализации цифровой повестки Евразийского экономического союза, утвержденное решением Коллегии Евразийской экономической комиссии от 19 февраля 2018 г. и др.

Основные выводы

1. В настоящее время полноценный цифровой суверенитет есть только у США. Все остальные страны не могут самостоятельно определять, что происходит в их цифровой сфере, кроме двух стран — России и КНР, которые приступили к суверенизации в сфере цифровых технологий.

2. Цифровые отношения, как и любые другие общественные отношения, могут быть (1) внутригосударственными

(частно-правовыми и публично-правовыми); (2) межгосударственными и (3) частноправовыми трансграничными.

3. К числу важнейших угроз в настоящее время относится высокий уровень зависимости России в сфере цифровых технологий, обусловленный, главным образом, полупериферийным характером российской экономики.

4. Цифровой суверенитет имеет значительную специфику и, прежде всего, включает в себя способность создать собственные технические средства и программное обеспечение, а также наличие поисковиков и социальных сетей.

Литература

1. Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: ключевые вызовы для мирового сообщества. — М.: Альпина Паблишер, 2016.

2. Дронов В. Ю. Международные и отечественные стандарты информационной безопасности. — Новосибирск: Издательство НГТУ, 2016.

3. Ефремов А. А. Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве // Информационное право. — 2016. — № 4. — С. 25–28.

4. Ефремов А. А. Развитие регулирования информационной или «цифровой» безопасности в документах международных организаций // Международное право и международные организации. — 2017. — № 1. — С. 48–55.

5. Ефремов А. А. Формирование единого цифрового пространства Евразийского экономического союза и обеспечение государственного суверенитета в информационной сфере // Евразийский юридический журнал. — 2016. — № 5. — С. 18–21.

6. Крайнова Н. А. «Международная цифровая безопасность»: миф или реальность? // Криминология: вчера, сегодня, завтра. — 2019. — № 4 (55). — С. 42–46.

7. Красинский В. В. Защита государственного суверенитета: монография. — М.: Норма, Инфра-М, 2017.

8. Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. — 2020. — № 9.

9. Нигматуллин Р. В. О противодействии угрозам и вызовам с позиции современного международного права // Юридический мир. — 2016. — № 11. — С. 54–58.

10. Тарасов А. М. Кибершпионы Duqu, Stuxnet, Flame, Gauss — что дальше? // Право и кибербезопасность. — 2012. — № 1. — С. 23–26.

11. Тарасов А. М. Киберугрозы, прогнозы, предложения // Информационное право. — 2014. — № 3. — С. 11–15.

12. Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе // Юридический мир. — 2016. — № 8. — С. 63–66.

13. Чернядьева Н. А. О международных подходах правового регулирования борьбы с кибертерроризмом // Информационное право. — 2016. — № 2. — С. 26–29.

14. Шишигин И. И., Николаева И. В. Кибербезопасность как основное направление развития правовых норм в условиях цифровой экономики: международные тренды // Научно-методический электронный журнал «Концепт». — 2019. — № 12. — С. 32–36.

15. Цибуля А. Н., Гордин В. А. К вопросу о состоянии информационной безопасности государства в условиях современных вызовов и угроз // Военно-юридический журнал. — 2014. — № 3. — С. 20–24.

Заключение

Право, являясь важнейшим регулятором общественных отношений, не может не реагировать на происходящие изменения в общественных отношениях. Цифровая трансформация общественных отношений обусловила необходимость принятия нормативных актов, закрепляющих позитивные последствия и минимизацию отрицательных последствий данного тренда. Формально юридически это привело к разработке в рамках права экономической безопасности нового института — права цифровой безопасности.

В настоящее время *словосочетание* «*цифровая безопасность*» *используется только в подзаконных актах*. Так, например, в государственном докладе Роспотребнадзора «Защита прав потребителей в Российской Федерации в 2016 году» говорится том, что цифровая грамотность — это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета. Она включает в себя цифровое потребление, цифровые компетенции и *цифровую безопасность*. В последнем докладе Роспотребнадзора использован термин «кибербезопасность».

Перефразируя известное утверждение К. Маркса об истории права («у права нет своей истории, отличной от истории общества»), можно сказать, что будущее права цифровой безопасности и цифрового права во многом зависит от развития информационных технологий. Это означает, что *прогнозирование перспектив развития права цифровой безопасности возможно во многом путем экстраполяции существующих технологических и экономических тенденций*.

Однако очевидно, что *влияние технологического фактора на развитие права цифровой безопасности корректируется правовой политикой государства в данной сфере общественных отношений*. А она определяется уже общественными факторами. Так, например, результатом резкого усиления геополитического противостояния является, в частности, принятие нормативного акта, именуемого *законом о социальных сетях* (ст. 10.6 федерального закона «Об информации, информационных технологиях и о защите информации»). Этим документом предусмотрено особое регулирование общения в сетях с посещаемостью более 500 000 пользователей в сутки.

Содержание законодательства о цифровой безопасности постоянно меняется. Поэтому необходимо отслеживать новую информацию в периодических изданиях. К числу наиболее информационно насыщенных следует отнести источники:

1) «Cnews» — ежемесячный журнал, посвященный телекоммуникациям, информационным технологиям и программному обеспечению[161];

2) «Вопросы кибербезопасности» — научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности[162];

3) журнал «Информационное право»[163].

Самой серьезной не решенной на сегодня задачей является определение *пределов цифровизации общественных отношений*. Существуют серьезные опасения перспектив так называемого цифрового рабства. По мнению председателя Конституционного суда РФ Валерия Зорькина, особая опасность исходит сейчас от цифровых технологий, которыми очень легко злоупотреблять и развитие которых без должного контроля со стороны общества чревато так называемой цифровой диктатурой[164].

---

[161] https://www.cnews.ru

[162] https://cyberrus.com

[163] https://infolaw.su

[164] Зорькин В. Возвращение государства // Российская газета. — 17.05.2021. — С. 3.

Учебное издание

Мансуров Гафур Закирович

Право цифровой безопасности

Учебник

Текст приводится в авторской редакции

16+

Ответственный редактор *С. Краснова*
Верстальщик *А. Мужилова*

Издательство «Директ-Медиа»
117342, Москва, ул. Обручева, 34/63, стр. 1
Тел./факс: +7 (495) 334-72-11
E-mail: manager@directmedia.ru
www.biblioclub.ru
www.directmedia.ru