

8. Алексеев, Н. Н. Основы философии права / Н.Н. Алексеев. – СПб.: Изд-во «Лань», 1999. – 256 с.
9. Джентиле, Э. Политические религии / пер. с итал. Ф. Станжевского. – СПб.: Изд-во «Владимир Даль», 2021. – 396 с.
10. Кошен, О. Малый народ и революция / пер. с франц. О.Е. Тимошенко; пред. И. Р. Шафаревича. – М.: Айрис-пресс, 2004. – 304 с.
11. Фёгелин, Э. Новая наука политики / пер. с англ. Н. Селивёрстова. – СПб.: Изд-во «Владимир Даль», 2021. – 372 с.

Мороз Наталия Олеговна
**ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ КАК ОСНОВА
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
РЕСПУБЛИКИ БЕЛАРУСЬ**

Белорусский государственный университет, доцент кафедры государственного управления, кандидат юридических наук, доцент, Nataliya.Maroz@gmail.com

Аннотация. В целях обеспечения должного уровня информационной безопасности особенно актуальным является вопрос выявления границ суверенной власти государства при осуществлении деятельности с использованием информационно-телекоммуникационных технологий. В этой связи настоящая статья посвящена выявлению сущности термина «информационный суверенитет» и соотнесение его с иными схожими понятиями, используемыми в международной практике.

Ключевые слова: информационный суверенитет; информационная безопасность; суверенитет; внутренние дела государства.

С учетом вызовов, с которыми столкнулось мировое сообщество в условиях пандемии, вопросы поддержания должного уровня информационной безопасности стали как никогда актуальными.

В настоящее время государственные органы Республики Беларусь, равно как и отдельные государственные служащие весьма часто подвергаются кибератакам. По оценкам Международного союза электросвязи Республика Беларусь занимает 89-ю позицию в мировом рейтинге кибербезопасности [1].

В таких условиях угрозы информационной безопасности не только традиционно рассматриваются в контексте национальной безопасности государства (п. 27, 34, 42 Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. №575), но и требуют самого пристального внимания со стороны государства.

В соответствии с п. 25 Концепции информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 г. № 1 (далее – Концепция) важнейшей целевой установкой обеспечения информационной безопасности Республики Беларусь является её информационный суверенитет.

В соответствии с п. 7 Концепцией под информационным суверенитетом понимается “неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность”.

Следует отметить, что сама концепция «информационного суверенитета», как и ее трактовка, отражает национальную систему официальных взглядов на данные вопросы. В международно-правовой доктрине, а также практике зарубежных государств используются и другие термины, которые хотя и имеют схожее содержание с понятием «информационный суверенитет», но все же не являются его синонимами.

Так, в частности, термин «информационный суверенитет», используемый в Концепции, следует отграничивать от «внутреннего суверенитета» в киберпространстве, рассматриваемого в таком авторитетном доктринальном источнике, как Таллинское руководство 2.0 по международному праву, применимому к кибероперациям (далее – Таллинское руководство). В соответствии с Таллиннским руководством внутренний суверенитет «предполагает суверенную власть государства в отношении кибер-инфраструктуры, лиц и кибер-деятельности, находящихся на его территории, в соответствии с его международными обязательствами» [2, с. 13].

Кроме того, в доктрине также используются такие термины, как «киберсуверенитет», «суверенитет киберпространства», «Интернет-суверенитет», «цифровой суверенитет».

Такое терминологическое разнообразие довольно четко демонстрирует отсутствие единого понимания концептуального аппарата в обсуждаемой области. Более того, единый подход отсутствует и к определению указанных выше понятий. Например, термин «киберсуверенитет» рассматривается в доктрине с разных точек зрения (как совокупность прав и обязанностей [3, с. 277–290], право «устанавливать контроль над нематериальным киберпространством в пределах территориальных границ» [4, с. 398] и т.д.).

К сожалению, в настоящее время государства не пришли к единому мнению о необходимости закрепления стандартов ответственного

поведения государства в киберпространстве в международном договоре универсального характера [5]. Таким образом, правоотношения в рассматриваемой сфере регламентируются нормами международного права общего характера. При этом ориентиры должного поведения государств в киберпространстве задаются нормами международной морали.

Наиболее авторитетными источниками норм международной морали в части определения правил ответственного поведения государств в киберпространстве являются отчеты Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций (далее – ГПЭ).

Важность принципа суверенитета в качестве основы для повышения безопасности в сфере использования информационно-телекоммуникационных технологий (далее – ИКТ) государствами подчеркивалась в отчете ГПЭ 2015 г., который наряду с отчетами ГПЭ 2010, 2013 гг. В частности, в отчете ГПЭ за 2015 г. указывалось, что «суверенитет государств и международные нормы и принципы, происходящие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях» [6].

С этой точки зрения необходимо отметить, что термин «информационный суверенитет» в меньшей степени направлен на определение границ суверенной власти Республики Беларусь в киберпространстве. В первую очередь, термин сформулирован в русле традиционного понимания суверенитета в международном праве.

Кроме того, полагаем, что понятие информационного суверенитета, закрепленное в Концепции, сформулировано с учетом содержания термина «внутренние дела», который традиционно рассматривается в контексте принципа невмешательства во внутренние дела. Отдельные аспекты содержания принципа, касающиеся информационного измерения внутренних дел, была сформулирована в Декларации о недопустимости вмешательства и вмешательства во внутренние дела государств, принятой Генеральной Ассамблеей ООН в 1981 г.

Взаимосвязь между понятиями «суверенитет» и «внутренние дела» была разъяснена Международным Судом ООН в решении по делу Никарагуа против США, который указал, что запрещенное вмешательство во внутренние дела государства должно иметь отношение к вопросам, в которых каждому государству разрешено свободно принимать решения на основании принципа государственного суверенитета. Один из них – это выбор политической, экономической, социальной и культурной системы, а также формулирование внешней политики» [7].

Полагаем, что содержание понятия «информационный суверени-

тет» соответствует положениям, сформулированным в отчетах ГПЭ за 2013, 2015 гг., а также не противоречит трактовке термина «внутренний суверенитет» в киберпространстве согласно Таллинскому руководству 2.0. В то же время Отчет ГПЭ и Таллинское руководство 2.0 рассматривают оба аспекта суверенитета, в то время как в Концепции не указываются территориальные границы суверенитета Беларуси в киберпространстве.

Такого рода неопределенность не способствует: во-первых, установлению четко определенного порога, когда поведение иностранного государства может рассматриваться в качестве нарушения суверенитета Республики Беларусь; во-вторых, укреплению международного доверия, на что, в том числе, ориентирована Концепция (статьи 23, 104 Концепции), поскольку позиция государства относительно территориальных пределов суверенитета в киберпространстве в данном случае не ясна.

Таким образом, понятие информационного суверенитета, впервые получившее закрепление в Республике Беларусь в Концепции информационной безопасности, в целом, отражает подходы, сложившиеся в доктрине, а также рекомендуемые ГПЭ для понимания сферы и объема действия государственной власти в киберпространстве.

Библиографические ссылки

1. Global Cybersecurity Index 2020 [Electronic resource] / International Telecommunication Union. – Mode of access: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. – Date of access: 15.09.2021.

2. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2nd Edition / ed. by Michael N. Schmitt. – Oxford: Oxford University Press, 2017. – 598 p.

3. Shen, Y. Cyber Sovereignty and the Governance of Global Cyberspace / Y. Shen // China Political Science Review. – 2016. – № 1. – P. 81 – 93.

4. Binxing, F. Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace / F. Binxing. – Beijing: Science Press Beijing, Springer, 2018. – 482 p.

5. Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (Advance copy) [Electronic resource]. – Mode of access: <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>. – Date of access: 23.10.2021.

6. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, A/70/174, 2015 [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: <https://undocs.org/ru/A/70/174>. – Дата доступа: 22.09.2021.

7. Military and Paramilitary Activities in and against Nicaragua (Nicaragua

Мороз Олег Васильевич
СТРАТЕГИЧЕСКАЯ ЭКОЛОГИЧЕСКАЯ ОЦЕНКА КАК
ЭФФЕКТИВНАЯ МЕРА ПО ОБЕСПЕЧЕНИЮ
КОНСТИТУЦИОННОГО ПРАВА КАЖДОГО НА
БЛАГОПРИЯТНУЮ ОКРУЖАЮЩУЮ СРЕДУ

Белорусский государственный университет, доцент кафедры экологического и аграрного права, кандидат юридических наук, доцент, moroz_ov@mail.ru

Аннотация. В публикации рассматриваются правовые критерии выделения объектов стратегической экологической оценки. Приводится отличие подходов к ее объектам в национальном законодательстве и Протоколе по стратегической экологической оценке к Конвенции об оценке воздействия на окружающую среду в трансграничном контексте.

Ключевые слова: стратегическая экологическая оценка; природоохранная мера; проекты стратегической (программной) документации; проектные решения; планируемая хозяйственная и иная деятельность; объекты; критерии.

В Республике Беларусь право каждого на благоприятную окружающую среду является одним из конституционных прав, что указывает на особое его значение. В соответствии со статьей 13 Закона Республики Беларусь от 26 ноября 1992 года № 1982-ХІІ «Об охране окружающей среды» оно обеспечивается, в том числе мерами по предотвращению вредного воздействия на окружающую среду, в качестве одной из которых следует рассматривать стратегическую экологическую оценку (далее – СЭО). Превентивный характер данной природоохранной меры во многом предопределяет ее эффективность, так как предупреждение вредного воздействия на окружающую среду представляется более рациональным чем его устранение.

Основной круг норм, регламентирующих СЭО, содержится в Законе Республики Беларусь от 18 июля 2016 года № 399-З «О государственной экологической экспертизе, стратегической экологической оценке и оценке воздействия на окружающую среду» (далее – Закон о ГЭЭ, СЭО и ОВОС) и Положении о порядке проведения стратегической экологической оценки, требованиях к составу экологического доклада по стратегической экологической оценке, требованиях к специалистам, осуществляющим проведение стратегической экологической оценки, утвержденным Постановлением Совета Министров Республики Бела-