3. перспективным направлением совершенствования института примирительных процедур в правовой системе Республики Беларусь представляется возможность внедрения в гражданское и хозяйственное судопроизводство предварительной независимой экспертной оценки, которая может быть использована в различных видах: предварительная нейтральная оценка (EarlyNeutralEvaluation), экспертиза по установлению фактических обстоятельств дела (Fact-Finding), экспертное определение (Expertdetermination), независимое разрешение (Adjudication) и др.

Библиографический список

1. Альтернативное разрешение споров : учеб. / под ред. Е. А. Борисовой. – М. : Издательский Дом «Городец», 2019. – 416 с.

2. Гражданский процессуальный кодекс Республики Беларусь, 11 янв. 1999 г., № 238-З: в ред. ЗаконаРесп. Беларусь от 17 июля 2020 г. № 45-З[Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

3. Здрок, О.Н. Медиация : пособие / О. Н. Здрок. – Минск : Четыре четверти, 2018. – 540 с.

4. Хозяйственный процессуальный кодекс Республики Беларусь : принят Палатой представителей 11 ноября 1998 г. : одобр. СоветомРесп. 26 ноября 1998 г. [Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.

5. Dispute resolution services [Electronic resource] / – Mode of access: https://iccwbo.org/dispute-resolution-services/docdex/docdex-expert/. – Date of access: 30/10/2020.

6. Expert determination [Electronic resource]. – Mode of access: https://www.wipo.int/amc/en/expert-determination/rules/. – Date of access: 30/10/2020.

ЭВОЛЮЦИЯ КЛЮЧЕВЫХ КОНЦЕПТОВ ПРАВА КИБЕРБЕЗОПАСНОСТИ

Ю.П. Гаврильченко
профессор кафедры финансового права и правового регулирования хозяйственной деятельности
Белорусского государственного университета,
доктор юридических наук, профессор

Цифровизация общественных отношений обусловливает стремительное развитие информационного права, при этом все более актуальными становятся вопросы правового обеспечения безопасности информационной среды. Число вредоносных объектов, которые обнаруживаются в сети ежегодно, исчисляется миллиардами, их распространение ведется более чем 100 миллионамиинтернет

адресов, и эти показатели ежегодно увеличиваютсяне менее, чем на 40% [1, с. 22]. При этом все чаще используются сложные элементы нападения, особую опасность составляют угрозы мобильным устройствам, которые ранее редко подвергались атакам. В литературе высказывается мнение о финансировании нападений в области киберпространства со стороны государственных органов некоторых стран [2, с. 30].

Несмотря на существующие проблемы, категория кибербезопасности остается одной из самых слабо разработанных в отечественной и зарубежной науке, в том числе правовой. По поводу ключевых понятий данной сферы отсутствует единообразие подходов.

В общем виде кибернетика (от греч. – «искусство управления») может быть определена наука об управлении, связи и переработке информации. К предметной области кибернетики относятся не только информационные, как полагают некоторые авторы [3, с. 99], но и и телекоммуникационные технологии. При этом управление подразумевает не наличие прямолинейных команд, а формирование и передачу таких сигналов, которые способны обеспечить стабильное развитие и устойчивость к возникающим угрозам.

Представляется ошибочной негативная конструкция определения кибербезопасности, согласно которой кибербезопасность предполагает защиту от максимального количества угроз. Данный термин целесообразнее определять в позитивном аспекте как обеспечение благоприятной среды для правомерной и успешной работы пользователей и систем в киберпространстве.

Некоторые авторы рассматривают кибербезопасность исключительно на уровне деятельности организации, полагая, что «основной целью кибербезопасности является упрощение программ, управляющих киберрисками, чтобы любая фирма могла позволить внедрить ее у себя» [4, с. 64]. Однако более обоснованно говорить о существовании разных уровней кибербезопасности: индивидуального [см., напр.: 5], коллективного (в том числе на уровне субъектов хозяйствования), государственного.

Международный стандарт ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности (ISO/ IEC 27032:2012 Informationtechnology - Securitytechniques - Guidelinesforcybersecurity) исходит из того, что киберпространство - сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей. Это высказывание может быть признано справедливым, но с оговоркой. Данная среда, рассматриваемая как в статическом (информация в ее цифровом представлении), так и динамическом понимании (информационное взаимодействие, специфическая деятельность), способна функционировать только при существовании соответствующего физического обеспечения (техническая инфраструктура, сами технологии, программное обеспечение, с помощью которых осуществляется реализация основных действий с информацией).

Технологическое обеспечение становится важнейшим условием создания безопасности киберсреды. В литературе отмечается, что уже в ближайшее время зависимость от иностранных производителей оборудования и разработчиков программного обеспечения может достигнуть критического уровня, поставив под угрозу саму возможность обеспечения кибербезопасности [2, с. 31]. В частности, власти Китая, несмотря на успехи в создании «Золотого щита» (Великий китайский файрвол), признали зависимость и незащищенность вследствие повсеместного использования программной платформы для мобильных устройств Android, основанной на «открытом» коде, но, как предполагается, подконтрольной специальным службам США [6, с. 131-132].

В подавляющем большинстве государств сложилась ситуация, при которой на каждом из участков информационно-коммуникационной инфраструктуры (чипы, схемотехника и т.п.) с высокой долей вероятности используются зарубежные решения с недостаточно изученной начинкой. Это явление оказывает положительное влияние на развитие экономики, ускоряя и удешевляя процессы, но создаёт угрозу национальной безопасности.

В литературе отмечается, что на постсоветском пространстве для понимания кибербезопасности, как правило, используют более широкое понятие информационной безопасности, под которым понимают состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие. При этом на Западе используют термин «кибербезопасность», под которым понимают надежность, устойчивость и неприкосновенность компьютерных сетей [7, с. 367]. Полагаем, такое жесткое разделение и чрезвычайно узкий подход к кибербезопасности утратили свою актуальность.

В 2000 г. Всекитайским собранием народных представителей была предпринята попытка определить классификацию возможных правонарушений в информационной сфере (постановление ВСНП по защите интернет-пространства). В результате выделены области, в которых могут осуществляться нарушения: экономическая, образовательная, сфера поддержания общественной стабильности и защиты граждан. Позднее известная британская компания составила рейтинг стран по уровню кибербезопасности, оценив не только традиционные показатели вроде процента зараженных вирусами устройств, но и такое важное условие, как своевременные изменения законодательства в данной области. Таким образом, кибербезопасность обретает все новые грани и аспекты.

В данном контексте нужно понимать, что конструктивные изменения законодательства обеспечивают защиту не только от киберпреступлений, но и от других киберугроз. В частности, в литературе исследуются такие новые угрозы, как кибертерроризм, сетецентрическая война, кибервойна [8].

Характерной особенностью кибертерроризма и его отличием от киберпреступности называются его масштаб, интенсивность, открытость и

последствия. В условиях разных подходов государств к вопросам кибербезопасности, а также использования киберпространства для продвижения политических интересов все более актуальными становятся проблемы кибервойн. «Почти сразу же после своего возникновения киберпространство превратилось в пятое (после земли, моря, воздуха и космоса) поле битвы различных политических и военных сил и продолжает оставаться таковым» [9, с. 152]. На февральской Мюнхенской конференции по безопасности 2018 г. Генеральный секретарь ООН А. Гутерреш призвал мировое сообщество приступить к серьезному обсуждению международного юридического режима, связанного с кибервойнами.

В условиях подобного противодействия все острее поднимается вопрос о защите киберсуверенитета. В 2015 г. в г. Учжэне на международной конференции по развитию Интернета Си Цзиньпин заявил, что Китай будет отстаивать свои национальные интересы в Интернете и не потерпит компромисса в вопросах обеспечения киберсуверенитета КНР.

Таким образом, концепция кибербезопасности разрастается, захватывая все новые аспекты социального взаимодействия. Это порождает необходимость исследования и детализации множества категорий и терминов, поскольку данный вопрос нуждается в самой серьезной и всесторонней проработке с учетом современных реалий.

Библиографический список

1. Безкоровайный, М.М., Татузов, А.Л. Кибербезопасность – подходы к определению / М.М. Безкоровайный, А.Л. Татузов// Вопросы кибербезопасности. – 2014. –№ 1. – С. 22-27.

2. Згоба, А.И., Маркелов, Д.В., Смирнов, П.В. Кибербезопасность: угрозы, вызовы, решения / А.И. Згоба и др. // Вопросы кибербезопасности. – 2014. –№ 5(8). – С. 30-38.

3. Томилов, И.О., Грицкевич, Е.В. Анализ актуальных киберугроз и средств защиты от них / И.О. Томилов, Е.В. Грицкевич// ИнтерэкспоГеоСибирь. – 2018. –С. 99-105.

4. Сафонова, М.Ф., Ципляева, С.А. Кибербезопасность: проблемы и решения / М.Ф. Сафонова, С.А. Ципляева// Естественно-гуманитарные исследования. – 2019.– № 24 (2). – С. 63-68.

5. Гольчевский, Ю.В., Некрасов, А.Н.К вопросу о кибербезопасности интернет-пользователей/ Ю.В. Гольчевский, А.Н. Некрасов // Известия ТулГУ, Технические науки, 2013.–Вып. 3. – С. 253-261.

6. Сейранова,С.Н. Киберугрозы как серьезный вызов национальной безопасности КНР / С.Н. Сейранова// Актуальные проблемы современных международных отношений. – 2017. –С. 131-136.

7. Ищанова, Р.К. Обеспечение кибербезопасности / Р.К. Ищанова // Большая Евразия: развитие, безопасность, сотрудничество. – 2019. – С. 367-368.

8. Булай, Ю.Г., Булай, Р.И. Профилактика и противодействие киберпреступности, а также международным киберугрозам/ Ю.Г. Булай, Р.И. Булай// Академическая мысль. –2017.– № 1. – С. 31-35.

9. Кардава, Н.В.Киберпространство как новая политическая реальность: вызовы и ответ / Н.В. Кардава // История и современность. – 2018. –№ 2. – С. 152-166.

ПРИНЦИП ДОБРОСОВЕСТНОСТИ МЕДИАТОРА

Д.В. Гапоненко
младший научный сотрудник
Национального центра законодательства и правовых исследований
Республики Беларусь

Процедура медиации, будучи эффективным способом урегулирования правовых конфликтов, притягивает внимание как отечественных, так и зарубежных исследователей. При этом востребованность данной процедуры в большинстве случаев напрямую зависит от степени реализации ее принципов, служащих основой оценки достижения социально значимых результатов.

Среди основополагающих принципов процедуры медиации законодатель Республики Беларусь выделяет принцип добросовестности, получивший отражение в положениях Закона Республики Беларусь от 12 июля 2013 года № 58-З «О медиации» (далее – Закон о медиации), Постановления Совета Министров Республики Беларусь от 28 декабря 2013 года № 1150 «Об утверждении правил проведения медиации» (далее – Правила проведения медиации) и Постановления Министерства юстиции Республики Беларусь от 17 января 2014 года № 15 «Об утверждении правил этики медиатора» (далее – Правила этики медиатора).

Обращаясь к трактовке термина «добросовестность», следует привести определение, отраженное в Юридическом словаре Блэка (Black’sLawDictionary), согласно которому добросовестность есть состояние ума, состоящая в честности в убеждениях или целях, верности своему долгу или обязательству, соблюдении разумных коммерческих стандартов добросовестности в торговле или бизнесе, или отсутствии намерения обманывать или искать недобросовестную выгоду [1, с. 307].

Среди явных нюансов национального правового регулирования медиативных отношений в контексте принципа добросовестности следует упомянуть о разрозненности положений правовых актов относительно субъектного состава. Так, согласно положениям ст. 3 Закона о медиации принцип добросовестности применим лишь в отношении сторон анализируемой процедуры, при этом п. 5 гл.1 Правил проведения медиации, п. 4 и п. 6 гл. 2 Правил этики медиатора относят принцип добросовестности к поведению и сторон процедуры, и медиатора [2; 3; 4].