УДК 34.05
ББК 67.404.9

ЦИФРОВЫЕ ТРАНСФОРМАЦИИ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНОЛОГИЧЕСКОГО СОТРУДНИЧЕСТВА И ВОПРОСЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНДУСТРИИ-4.0*

М. В. Шугуров
Саратовская государственная юридическая академия (Саратов, Россия)

Статья посвящена анализу тенденций и перспектив цифровых трансформаций международного научно-технологического сотрудничества в процессе перехода к Индустрии-4.0. Автор поднимает вопрос о роли и месте безопасности цифровых коммуникаций и цифровых инфраструктур международного сотрудничества в рассматриваемой сфере в общем контексте обеспечения международной информационной безопасности. В свою очередь все это рассматривается в качестве аспекта перехода к устойчивому развитию и достижению его целей, что означает реализацию межсекторального подхода. Обосновывается, что международное научно-технологическое сотрудничество может стать драйвером перехода к устойчивому развитию только в условиях кибербезопасности. На основе изучения актов «мягкого» и «твердого» международного права, а также результатов деятельности международных организаций и рабочих групп автор приходит к выводу о том, что концептуальные положения глобальной стратегии устойчивого развития еще в недостаточной мере нашли свое отражение в международном праве информационной безопасности. В исследовании обосновывается конвергенция данных предметных областей на основе привлечения аргумента о том, что ИКТ играют существенную роль в достижении целей устойчивого развития. Соответственно, их распространение, особенно в развивающиеся страны, способно привести к сокращению глобального цифрового разрыва, но только при условии обеспечения надлежащего уровня информационной безопасности. Основной вывод статьи заключается в обосновании необходимости включения в состав международного сотрудничества в сфере науки и технологий такого направления, как обеспечение информационной безопасности его основных форм. Данный вывод экстраполируется на региональное научно-технологическое сотрудничество в рамках ЕАЭС, которое должно быть максимально интегрировано в реализацию Цифровой повестки Союза, придающей повышенное внимание информационной безопасности.

Ключевые слова: ИКТ, цифровой разрыв, информационная безопасность, цифровая экономика, международное сотрудничество в научно-технологической сфере, Индустрия-4.0, развивающиеся страны, Евразийский экономический союз.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20–011–00780 («Модель правового регулирования научно-технологической и инновационной интеграции в рамках ЕАЭС и вызовы Четвертой промышленной революции»).

DIGITAL TRANSFORMATION OF INTERNATIONAL COOPERATION IN SCIENCE AND TECHNOLOGY AND THE ISSUES OF LEGAL ENSURING OF INTERNATIONAL INFORMATION SECURITY IN CONDITIONS OF INDUSTRY-4.0

M. V. Shugurov
Saratov State Law Academy (Saratov, Russia)

The present article is devoted to analyzing the role and significance of international information security and its legal regulation in a process of transition to sustainable development. Based on examining the acts of «soft» and «hard» international law and also on results of activity of international organizations and working group, the author concludes that conceptual provisions of the global strategy of sustainable development are reflected in international law of information security incompletely. The study substantiates a convergence of these subject areas by arguments that ICT are key factors of achieving the Sustainable Development Goals. Accordingly, transfer of ICT and dissemination thereof in, especially, developing countries can lead to reducing the global digital divide but under one condition. The latter is an ensuring the proper level of information security. Much attention is paid to mean of information security for transition to Industry-4.0 corresponding the SDG No 9.

Keywords: sustainable development, ICT, information security, digital divide, digital economy, international cooperation, Industry-4.0, developing countries.

Doi: https://doi.org/10.14258/ralj(2020)4.10

Динамичные процессы революционного перехода к новому этапу промышленного и технологического развития, понимаемого как Индустрия 4.0, открывают новые перспективы и формируют новые задачи для международного сотрудничества в сфере инноваций, науки и технологий (далее — МИНТС) на универсальном и региональном уровнях. Как известно, Индустрия 4.0 предполагает самое широкое использование различных цифровых технологий в процессе организации и осуществления производственного цикла. В настоящее время все это коррелирует цифровой трансформации научно-технологического сотрудничества. Напомним, что важнейшей формой МИНТС является обмен научной информацией и данными. Это предусмотрено как в многосторонних межгосударственных договорах, так и в двусторонних межправительственных соглашениях по научно-техническому сотрудничеству.

Данного рода сотрудничество следует рассматривать как составную часть сотрудничества государств в информационной сфере. Одновременно информационное взаимодействие пронизывает и другие формы МИНТС — совместные исследования и разработки, обмен специалистами, передачу технологий и т. д. Для всех форм взаимодействия все более актуальным становится развитие информационной структуры, позволяющее осуществлять цифровую трансформацию сотрудничества. Например, в сфере передачи технологий — разнообразные платформы на основе использования ИКТ (например, платформа «зеленая ВОИС»). Если говорить в целом, то расширенное использование цифровых технологий (в особенности искусственного интеллекта и компьютерного анализа текста и данных) не только повышает результативность научной и научно-технической деятельности в рамках совместных проектов и программ, но и повышает эффективность организации международного взаимодействия.

Наиболее динамично цифровые трансформации МИНТС происходят на уровне региональных объединений государств, что находит свое отражение в запуске разнообразных цифровых платформ и сервисов (например, Европейское облако открытой науки, Цифровой платформы инновационного сотрудничества СНГ), которые могут рассматриваться как важнейшие инфраструктурные объекты общего научно-технологического пространства. В данном направлении работают и международные организации. Укажем на платформы инновационной политики ОЭСР и Всемирного банка при осуще-

ствлении деятельности по развитию единого информационно-аналитического ресурса в сфере науки, технологий и инноваций. Достаточно перспективной является цифровая трансформация региональных технологических платформ и сетей трансфера технологий, являющихся драйверами технологического перевооружения экономики и общества.

Нет никаких сомнений, что «цифровизация» представляет собой своего рода ускоритель научно-технологической интеграции на региональном уровне и, соответственно, является инструментом ее расширения и углубления. В этой связи можно констатировать, что развитие МИНТС теснейшим образом сопряжено не только с региональной промышленной политикой, но и с реализаций региональных цифровых повесток. Все сказанное самым непосредственным образом актуально для Евразийского экономического союза (далее — ЕАЭС), перед которым стоят серьезные задачи по технологической модернизации в условиях Четвертой промышленной революции, а также задачи цифровой трансформации пространства научно-технологической и инновационной кооперации и интеграции. В частности, если обратиться к анализу такого содержания деятельности АНО «Научный центр евразийской интеграции» [1], как «наука и образование», то в качестве одной из задач выдвигается создание условий для прорывного научно-технологического развития России и стран-членов ЕАЭС за счет запуска евразийского сетевого междисциплинарного взаимодействия в единой информационной цифровой среде, облегчающей процесс: от проведения совместных прикладных научных исследований и экспериментальных разработок для индустриализации (коммерциализации — М. Ш.) научно-прикладных идей.

В наиболее обобщенном виде перспективным и одновременно инновационным направлением развития МИНТС является формирование информационной инфраструктуры и на его основе — информационного пространства. Вовлечение в широкое использование цифровых технологий позволит не только повысить эффективность исследований и разработок, но и усилить эффективность сотрудничества. Позитивные результаты цифровых трансформаций возможны здесь в случае надежности и безопасности цифровых решений. Как думается, сотрудничество в сфере цифровых трансформаций МИНТС в дальнейшем станет предметом правового регулирования на межгосударственном и межправительственном уровне.

Однако помимо правового обеспечения продвижения цифровых решений в рамках реализации разномасштабных научно-технологических проектов и программ как в составе международно-договорного сотрудничества, так и вне его, в том числе продвижения данных решений в рамках глобальных исследовательских (мега) инфраструктур мегасайенс, актуализируется вопросы нейтрализации специфических вызовов и рисков, которые, впрочем, характерны для любых цифровых пространств. Речь идет о том, что «цифровое» пространство сотрудничества в сфере науки, технологий и инноваций может подвергаться достаточно разрушительные киберугрозам. Отсюда возникает новый предмет общей заинтересованности — информационная безопасность (или кибербезопасность) как аспект современного МИНТС в целом и региональной научно-технологической интеграции в частности.

В свете сказанного позитивные цифровые трансформации рассматриваемого направления международного сотрудничества объективным образом сопрягаются с общими вопросами обеспечения международной информационной, или кибербезопасности. Эти вопросы рассматриваются на универсальном и региональном уровнях. В последнем случае как в ЕС, так и в ЕАЭС повышенное внимание в рамках интеграционных процессов уделяется вопросам информационной безопасности, что является одним из приоритетов региональных цифровых повесток.

В случае ЕАЭС развертывание цифровой интеграционной платформы и обеспечение интероперабельности в рамках Союза нацелено на формирование общего цифрового экономического пространства и развития цифровой экономики. Формирование общего научно-технологического пространства, да еще в цифровом формате, здесь представляет собой не менее значимую задачу. Однако в обоих случаях развитие телекоммуникационных сервисов и высокоскоростных сетей, а также представление высокопроизводительных облачных сервисов должно предполагать обеспечение не только интероперабельности, но и кибербезопасности.

Сотрудничество и его наиболее «продвинутая» форма — интеграция — в сфере науки, технологий и инноваций предполагает коммуникативные процессы (коллаборацию), которые осуществляются между участниками данного направлений сотрудничества в ходе реализации совместных программ и проектов на основе функционирования научно-исследовательских сетей, технологических

платформ, сетей трансфера технологий и т. д. Сетевая природа и черты виртуальности, присущие научно-технологической коммуникации, нашли свое развернутое обоснование в литературе [2–5].

Вполне очевидно, что цифровые трансформации МНТС в целом и научно-технологической интеграции в частности предполагают разновекторный баланс между генерированием научной и научно-технологической информации, ее распространением и использованием. Конечно, проникновение цифровых технологий во все формы взаимодействия участников научно-технологической интеграции многократно повышает эффективность сотрудничества в сфере НИОКР и коммерциализации полученных результатов. Одновременно это приводить к удорожанию НИОКР, а также создает риски, связанные с использованием цифровых технологий и ИКТ-систем, которые широко используют виртуализацию, облачные хранилища данных, разнородные технологии связи и оконечные устройства. Однако именно с помощью данного рода технологий вполне можно обеспечить локализацию и ограничение киберугроз в научно-технологическом пространстве. В конечном счете это может привести к окупаемости использования средств, затрачиваемых на обеспечение кибербезопасности.

Из сказанного проистекает вывод о том, что в условиях Индустрии 4.0 актуализируется проблема обеспечения информационной безопасность не только национальных научно-технологических комплексов, подвергающихся цифровым трансформациям, но и инфраструктуры международной коллаборации, и региональной научно-технологической и инновационной интеграции. Защищенность цифровых процессов в рассматриваемой сфере достигается за счет развития технологий безопасного хранения, обработки и анализа данных, включая вопросы идентификации личности и методы защиты персональных данных.

Но все же кибербезопасность МИНТС во многом зависит от решения вопросов достижения всеобщей кибербезопасности. Это в очередной раз доказывает, что вопросы развития системы международной информационной безопасности, в том числе значение, характер и перспективы ее международно-правового регулирования, имеют «сквозной» характер. В настоящее время данная проблематика обсуждается на уровне государств, межгосударственных объединений, международных межправительственных и неправительственных организаций. Обеспечение международной информационной безопасности, а равным образом развитие соответствующего международно-правового института привлекает к себе внимание не только субъектов международного права, но и значительное количество негосударственных акторов — цифровых компаний, ассоциаций, общественных движений и, наконец, внимание экспертного, а также научного сообщества, количество аналитических и исследовательских результатов деятельности которого растет по экспоненте [6, 7]. Несомненно, представители научно-академических кругов и представители сектора НИОКР не только могут, но и должны рассматриваться в качестве стейкхолдеров данных обсуждений. Степень значимости данной проблематики многократно увеличилась по причине коренных изменений, связанных с ускоренной цифровизацией общества и экономики, а также с широкими масштабами распространения цифровых технологий, являющихся основой Индустрии-4.0, но одновременно выступающих источниками ее рискогенного характера.

Заметим, что цифровое лидерство тех или иных государств, а также их региональных объединений, означающее получение достойных дивидендов от цифровизации экономики и общества, предполагает достижение высокой степени их информационной безопасности, в том числе безопасности их научно-технологической инфраструктуры.

Как отмечается в одном из специальных докладов Генерального секретаря ООН, распространение цифровых технологий несет с собой не только выгоды, но и угрозы. При этом новейшие цифровые технологии могут принести пользу странам только в случае, если они располагают качественной цифровой (в особенности наличие широкополосной связи) и дополнительной (энергетическая инфраструктура, человеческий капитал, нормативно-правовые рамки) инфраструктурами [8]. Формирование и развитие данной инфраструктуры можно рассматривать как новое направление не только международной производственной, но научно-технологической кооперации.

В условиях ускоренной цифровизации, приводящей к расширению объемов цифрового пространства, а также к разрастанию среды, представленной объектами информационной инфраструктуры при одновременном увеличении количества кибератак, статистика которых приведена в одном из аналитических документов ЕС, весьма значимым направлением приложения совместных усилий всех заинтересованных сторон становится дальнейшее развитие концепции международной ин-

формационной безопасности, включая концепцию соответствующего международно-правового института. С точки зрения предмета нашей статьи это должно найти в дальнейшем свое преломление во включении в стратегии и программы в сфере МИНТС вопросов сотрудничества в сфере кибербезопаосности. Однако, с нашей точки зрения, разработка данного рода направления сотрудничества во многом привязана к концептуальным, нормативно-правовым и практическим аспектам института международной информационной безопасности.

О важности концептуального аспекта международной информационной безопасности и, соответственно, ее правового регулирования, а также дальнейшей разработки концептуальных подходов к ее правовому обеспечению говорится не только в научной литературе [9, p. 85–91; 10–12], но и в Разделе VII широко известного Доклада Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2015 г. Так, в п. 30 (а) Группа сочла необходимым признать важность мер по дальнейшему развитию государствами на совместной и индивидуальной основе концепций международного мира и безопасности в сфере использования ИКТ на правовом, техническом и политическом уровнях [13].

К одному из наиболее известных направлений концептуального поиска относится обоснование возможности перехода к многостороннему, т. е. универсальному международно-правовому регулированию международной информационной безопасности. В перспективах такого сценария развития рассматриваемого института международного информационного права уверены ряд государств, включая Россию, а также значительная часть представителей юридической науки, том числе международно-правовой.

В свою очередь, хотелось бы уделить внимание такому аспекту развития международно-правовой концепции международной безопасности, как междисциплинарность, или точнее сказать, межсекторальность. Рассмотрение данной межсекторальности позволит по-новому взглянуть на содержание и цели информационной безопасности МИНТС. В достаточно тезисной форме это означает такое направление концептуализации, как включение в повестку международно-правового сотрудничества по развитию института международной информационной безопасности ряда вопросов, например, формирование у населения навыков и умений поведения в информационной среде, а также формирования навыков трудовой деятельности в условиях Индустрии — 4.0 [14]. Все это должно найти свое продолжение в сотрудничестве по выработке цифровых компетенций у исследователей и субъектов научно-технической деятельности.

В литературе совершенно верно указывается на то, что университеты, которые инвестируют в цифровые компетенции сотрудников, получают целый ряд преимуществ, а именно — повышение конкурентоспособности сферы услуг в сфере высшего образования на основе использования цифровых платформ и технологий, например, анализа больших данных и т. д. [15, с. 200]. Но, как нам представляется, формирование цифровых компетенций сотрудников должно не только преследовать интересы развития онлайнового рынка образовательных услуг, но и интересы достижения цифровой трансформации взаимодействия науки и образования, с одной стороны, и производства — с другой, а также расширения использования возможностей цифровых технологий в сфере прикладных и фундаментальных исследований. Скажем больше, весьма перспективным является использование цифровых решений и для оптимизации интеграции научно-образовательных систем в рамках интеграции науки, образования и производств на уровне регионального объединения государств как такового.

Следует напомнить, что одним из ключевых для настоящего времени является «зеленый» вектор НТП, направленный на обеспечение перехода к устойчивому развитию на основе экологически обоснованных технологий. К тому же Индустрия 4.0 также предполагает не только цифровизацию, но и экологизацию производства. В этом свете следует выдвинуть идею масштабного междисциплинарного аспекта, такого как вопрос о содержательной связи между международной информационной безопасностью как таковой и ее правового обеспечения, с одной стороны, и Повесткой дня в области устойчивого развития на период до 2030 г. — с другой (далее — Повестка-2030) [16]. Данная Повестка является *Глобальным планом действий*, который сегодня активно реализуется на универсальном, региональном и национальном уровнях. Повышенная активность в сфере мониторинга достижения семнадцати Целей устойчивого развития (далее — ЦУР) и соответствующих целевых задач, предусмотренных в Повестке-2030, характерна для региональных объединений государств, в том числе не только для ЕС, но и ЕАЭС, который также, как известно, осуществляет также реализацию Цифро-

вой повестки и заинтересованно относится к вопросам достижения информационной безопасности. На универсальном уровне постоянный мониторинг хода достижения ЦУР осуществляет Генеральный секретарь ООН, в своем докладе за 2019 г. отмечающий необходимость обеспечения доступа к новейшим технологиям, в том числе технологиям использования больших данных при одновременном указании на необходимость избегать связанных с ними подводных камней посредством развития человеческого потенциала и профессиональных навыков [17]. Укажем, что в Повестке-2030 указываются различные технологии, призванные стать основой достижения ЦУР. При этом в качестве ключевых указываются ИКТ, имеющие, по сути, «сквозной» характер. Это усиливает значимость обеспечения безопасности тех пространств, где они используются, включая пространство МИНТС.

Поэтому исходным условием осуществления отмеченного нами междисциплинарного подхода в качестве импульса для развития соответствующего международно-правового института может выступить признание значимости ИКТ, а также доступного и безопасного Интернета для развития, в том числе для устойчивого развития. Данный подход характерен и для самой Повестки-2030, признающей, что распространение ИКТ и осуществление глобального подключения сетей открывают огромные возможности для преодоления цифрового разрыва и формирования общества знаний. Так, ЦУР № 17.8 предусматривает расширение использования высокоэффективных технологий, в частности ИКТ. Это дополняет ЦУР № 17.7, предусматривающую политические обязательства по разработке и передачи экологически безопасных технологий в развивающиеся страны на благоприятных и взаимно согласованных условиях. ИКТ расценивается как ключевой фактор решения ряда задач, например, образование и стипендии (задача 4a), расширение прав и возможностей женщин (задача 5b), не говоря уже о ссылках на ИКТ в целевых задачах в сфере обеспечения экономического роста, энергоэффективности и водоснабжения, а также адаптации к климатическим изменениям. В дополнение к этому тематические резолюции ГА ООН «Использование информационно-коммуникационных технологий в целях устойчивого развития» постоянно указывают на необходимость обеспечения безопасности при использовании ИКТ. Кроме этого, как об этом свидетельствует преамбула резолюции ГА ООН 74/35 от 12 декабря 2019 г., ИКТ отнесены к технологиям, разработка, передача и использование которых имеет самое непосредственное отношение к международной безопасности в целом [18].

Одновременно нельзя обойти стороной универсальный консенсус, достигнутый в формате ООН по вопросам международной информационной безопасности, который является основой для Рекомендаций о нормах, правилах и принципах ответственного поведения государств в киберпространстве 2015 г., выработанных Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникациям в контексте международной безопасности. В основе концепции, которой придерживается Группа, — положение о том, что ИКТ могут являться одним из факторов ускорения прогресса на пути развития (п. 30). Однако в свете современной парадигмы развития данное положение должно подлежать конкретизации в направлении понимания роли ИКТ именно как фактора перехода к устойчивому развитию и своевременному достижению ЦУР. Смену парадигм можно видеть не только в документах международных организаций, но и в доктрине, когда на смену работам о важности ИКТ для развития [19] приходят работы о роли ИКТ для устойчивого развития [20].

Рассматриваемое нами направление развития концепции международной информационной безопасности и ее правового обеспечения в направлении «погружения» в наиболее широкую по своему содержанию проблематику глобального перехода к устойчивому развитию, важными средствами которого являются «устойчивые технологии, как думается, в определенном смысле даже выходит за рамки обозначенного межсекторального подхода. Это связано с тем, что международная информационная безопасность может быть рассмотрена как часть в системе целого, а именно как часть международной безопасности, являющейся фундаментальным условием устойчивого развития и, что само по себе разумеется, важнейшим условием для реализации международно-признанных прав и свобод человека, что является одной из парадигмальных основ Повестки-2030.

Поэтому результатами предлагаемого нами концептуального подхода может выступить:

1. Достижение понимания того, что международная информационная безопасность является средством для достижения глобальных цивилизационных целей. В частности, ЦУР № 10 предполагает формирование справедливого и безопасного миропорядка, в том числе основанного на сокращении неравенства межу государствами и внутри них. Вполне очевидно, что ориентиры ЦУР № 10

можно рассматривать как условия для достижения всех других ЦУР, предполагающих, в том числе, задачи распространение ИКТ в том или ином секторе перехода к устойчивому развитию. Действительно, устойчивое развитие возможно только в условиях открытой, безопасной, стабильной и мирной ИКТ-среде. Одновременно, именно такое качество информационной среды может стать залогом эффективного МИНТС, являющегося, как мы уже сказали, фактором перехода к устойчивому развитию. Только в этом случае возможна реализация преимуществ Индустриии-4.0, как и сам переход к ней в формате устойчивого развития. Все это имеет непосредственное отношение к ЦУР № 9 «Устойчивая индустриализация», предполагающая в качестве задачи 9 (с) развитие инфраструктуры всеобщего и недорогого доступа к Интернету. В связи с этим вполне обоснованными являются рекомендации к обеспечению кибербезопасности Индустрии 4.0 в контексте стратегии устойчивого развития [21, 22].

2. Развитие международного информационного права в целом и международно-правового института международной информационной безопасности в частности в направлении их включения в так называемое «международное право устойчивого развития» (*international law of sustainable development*), представленного в настоящее время совокупностью норм и принципов международного экологического, международного экономического права и международного права прав человека.

В целом именно необходимость своевременного достижения ЦУР во всех странах вполне можно рассматривать как важнейший дополнительный фактор развития международно-правового института международной безопасности и его концепции. Одновременно внесем некоторые уточнения. Так, в п. 2 резолюции ГА ООН 71/28 Ассамблея высказала положение о том, что целям возможных стратегий по рассмотрению угроз в информационной сфере может служить продолжение изучения соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем [23]. На наш взгляд, в отличие от данных концепций развиваемый нами подход к международной информационной безопасности в контексте стратегии устойчивого развития говорит не столько о *средствах* обеспечения данной безопасности, а о том, каково ее *предназначение*. Исходя из данного тезиса, сформулируем вопрос о том, эксплицируется ли рассматриваемый нами междисциплинарный аспект на уровне аналитических работ и различных международных площадок? На этот вопрос надо ответить положительно. Это показывает обоснованность и эвристическую ценность предлагаемого нами подхода к направлению развития концепции международной информационной безопасности и ее правового регулирования.

Несмотря на то, что в самой Повестке-2030 проблематика информационной безопасности для устойчивого развития не затрагивается, она является неотъемлемой частью глобальной стратегии устойчивого развития, что можно обосновать признанием значения ИКТ для устойчивого развития и достижения его целей. На наш взгляд, именно контекст устойчивого развития позволяет говорить о единстве безопасности и инклюзивности цифрового мира, в который все более погружается научно-технологическое развитие и МИНТС. Это особенно важно для развивающихся стран, перспективы развития которых связаны с вовлечением в цифровые процессы и трансформации, выгода от которых будет получена только в случае сокращения цифрового неравенства и обеспечения необходимого уровня информационной безопасности. Первый аспект наиболее явно прослеживается в докладе ЮНКТАД 2019 г. о развитии цифровой экономики в глобальном мире в аспекте достижения ЦУР [24]. Второй же аспект актуализируется на других площадках, например, на уровне Международного союза электросвязи (далее — МСЭ), под эгидой которого функционирует Глобальный форум по кибербезопасности. К сожалению, как это можно заключить из анализа специальной литературы по преодолению глобального цифрового разрыва [25], в процессе соответствующего международного сотрудничества вопросы содействия обеспечению информационной безопасности здесь зачастую не затрагиваются.

Поэтому неслучайно, что проблематика информационной безопасности развивается в научной среде и обсуждается на международных симпозиумах, посвященных устойчивому развитию [26–28]. Весьма динамично на данный концептуальный запрос откликнулась ОБСЕ, исходящая из современного понимания международной безопасности именно в контексте устойчивого развития [29].

Межсекторальный подход к международной информационной безопасности разделяется и всесторонним образом развивается в рамках Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS). Это стало возможным благодаря включению повестки развития

информационного общества в контекст Повестки-2030. Кроме этого, Всемирная встреча заявила подход к рассмотрению кибербезопасности сквозь призму достижения ЦУР, в частности ЦУР № 9 [30]. Далее на встрече в 2018 г. одна из панельных сессий прямо была посвящена вопросам анализа наилучших практик в сфере кибербезопасности для достижения ЦУР [31]. На данной сессии были представлены подходы ряда специализированных учреждений ООН, что говорит о развитии их киберстратегий.

Несмотря на концептуальную интеграцию концепции международной информационной безопасности и концепции устойчивого развития, предпринятую в экспертной среде и в рамках международных организаций и форумов, международно-правовая база в сфере международной информационной безопасности, представленная источниками «твердого» и «мягкого» права, данный междисциплинарный аспект пока что учитывает не в полной мере. Аналогичная ситуация характерна для правового регулирования МИНТС. Это затрудняет окончательное отнесение международного информационного права к «международному праву устойчивого развития», в котором, как известно, большое внимание уделяется вопросам МИНТС. Это можно рассматривать в качестве недостатка правового обеспечения перехода к устойчивому развитию.

Тем не менее здесь налицо определенные новеллы. Обращает на себя внимание то, что Декларация глав государств Британского содружества наций 2018 г., посвященная вопросам поддержки развития киберпространства [32], в том числе в формате совестных усилий, в разделе 1 «Киберпространство, содействующее экономическому и социальному развитию и онлайновым правам», в качестве исходного содержит положение о том, что открытое, инклюзивное и безопасное киберпространство выступает «двигателем» для достижения Целей устойчивого развития во всем Сообществе. В свою очередь, в Парижском призыве, принятом в 2018 г. на высшем уровне Глобального форма по управлению Интернетом [33], хотя о целях устойчивого развития не говорится, но вполне заметно присутствует холистический подход, согласно которому стабильное и мирное киберпространство стало составной частью жизни во всех ее аспектах, а именно социальном, экономическом, культурном и политическом.

Если перейти к анализу актов международного права, содержащих юридически обязательные положения, то необходимо уточнить, что они представлены главным образом двухсторонними договорами и региональными соглашениям, что отражает текущую правовую специфику международно-правового института международной информационной безопасности. Специально отметим, что в единственном проекте универсального международного правового акта — концепции Конвенции об обеспечении международной информационной безопасности [34], предложенной Россией, к сожалению, интересующий нас междисциплинарный подход не отражен. Если обращаться к двусторонним или региональным соглашениям, участником которых является Россия [35, с. 40–42], то интересующий нас межсекторальный аспект в них также не выражен. Однако несомненно, что обеспечение информационной безопасности критически важных объектов государств в качестве одного из направлений сотрудничества, предусмотренного в ст. 3 (8) Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в сфере международной информационной безопасности 2013 г., в принципе, может включать в себя обеспечение информационной безопасности объектов научно-технологической инфраструктуры.

Среди региональных актов наиболее известным договором является Африканская конвенция о кибербезопасности и защите персональных данных [36]. К сожалению, проблематика устойчивого развития в ней также не затрагивается, хотя при этом конечно данная Конвенция вносит свой вклад в создание условий для формирования цифровой экономики на Африканском континенте и может рассматриваться как инструмент для достижения ЦУР № 8 и № 9.

Одновременно со всем сказанным необходимо обозначить связь между международно-правовым институтом международной информационной безопасности и ЦУР № 17, предполагающей передачу технологий как одного из средств по обеспечению всех остальных ЦУР. Конечно, в данной ЦУР говорится о передаче экологически устойчивых технологий, однако, в силу решающей роли ИКТ для обеспечения развития, их передача и распространение — важнейшей условие преодоления цифрового разрыва, что должно дополняться содействием укреплению потенциала развивающихся стран в сфере профессиональной подготовки, на что соответствующее внимание обращается в тематических резолюциях ГА ООН.

Рассматривая перспективное направление развития интересующего нас международно-правового института, отметим, что, несмотря на успехи на универсальном уровне при одновременной «пробуксовке» в решении вопроса о принятии юридически обязательных актов универсального характера, данный институт развивается на региональном уровне. В связи с этим возникает новое направление исследований, связанное с изучением прямой и обратной связи между повестками и стратегиями в сфере кибербезопасности тех или иных межгосударственных объединений и альянсов государств (ЕС, ЕАЭС, БРИКС, ШОС, СНГ, Группа 20 и др.) [37] и их повестками в сфере устойчивого развития, которые оказывают влияние на содержательную трансформацию МИНТС, функционирующего их рамках. Все это должно быть дополнено исследованием подходов к данной междисциплинарной связи в рамках международных организаций соответствующего профиля, например, Международного союза электросвязи.

К сожалению, данные повестки существуют пока параллельно, что как раз и не позволяет осуществить «плотное» включение проблематики информационной безопасности в состав МИНТС. Исключением здесь не является также и ЕС, в котором вопросы устойчивого развития не рассматриваются в повестке кибербезопасности [38], а также не затрагиваются на уровне наднационального регулирования данной сферы общественных отношений [39]. В свою очередь проблематика кибербезопасности еще не вошла в Повестку ЕС в области устойчивого развития. Напомним, что первое Сообщение Комиссии о последующих шагах для устойчивого будущего Европы [40] свидетельствовало о том, что ответ ЕС на Повестку-2030 будет включать два направления работы: 1) интеграция ЦУР в содержательные рамки европейской политики и текущие приоритеты Комиссии; 2) осмысление дальнейшего развития долговременных перспектив и сосредоточение на секторальных стратегиях после 2020. Тем не менее Повестка ЕС в области устойчивого развития, тесно связанная со стратегией Единого цифрового рынка, косвенным образом предполагает надежный уровень кибербезопасности. Отсюда следует сделать вывод о косвенном соотношении между цифровой повесткой ЕС, задающей содержательные рамки регионального МИНТС в формате Инновационного союза, и его повесткой в сфере кибербезопасности. Интерес также вызывают рекомендации Агентства ЕС по кибербезопасности (ENISA) в отношении обеспечения кибербезопасности в условиях Индустрии 4.0 [41], что также косвенным образом связано с повесткой ЕС в области устойчивого развития.

В ЕАЭС, как можно судить по Цифровой повестке Союза [42], проблематика цифровых трансформаций также не сопряжена с интеграционными усилиями по достижению ЦУР. В данном документе говорится лишь об обеспечении устойчивого функционировании единого информационного пространства. Более того, Повестка ЕАЭС в области устойчивого развития в отличие от ЕС, к сожалению, еще не сформирована, но тематика перехода к устойчивому развитию стала традиционным направлением интеграционного взаимодействия. То обстоятельство, что обеспечение безопасности единого информационного пространства является одним из приоритетов Цифровой повестки Союза, может оказать положительное воздействие на ускорение научно-технологической интеграции и ее «развороте» в направлении достижения целей устойчивого развития. Это связано с тем, что формирование возможной цифровой интеграционной платформы ЕАЭС предполагает не только обеспечение интероперабельности, развитие телекоммуникационных сервисов и высокоскоростных сетей, высокопроизводительных облачных сервисов в рамках Союза и одновременно в рамках эффективно взаимодействующих национальных платформ позволит сформировать общее цифровое экономическое пространство, которое должно обладать высокой степенью кибербезопасности.

Если говорить в целом, то в настоящее время режим международной информационной безопасности достаточно фрагментирован, хотя на региональном уровне начинают формироваться достаточно эффективные правовые режимы. Думается, что именно его включенность в стратегию устойчивого развития позволяет актуализировать фактор по привнесению в него большей системности, что далее будет благоприятно сказываться на формировании безопасной киберсреды среды МИНТС, вписывающегося в контур «зеленого» НТП.

Как бы то ни было, пример реализации междисциплинарного подхода подает ООН — главный флагман реализации стратегии устойчивого развития. К сожалению, это не всегда принимается во внимание в научной литературе, в которой зачастую деятельность данной универсальной международной организации анализируется вне обращения к другим направлениям ее активности [43]. Как таковой межсекторальный подход ООН имеет место и проявляется в разных направлениях. Ука-

жем на учреждение рабочей *Группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (OEWG),* которая должна дополнить работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. В данном случае речь идет о дополнении государственно-центричного подхода подходом мультистейкхолдерским, обоснованным ОЭСР и апробированным в ЕС. Он заключается в управлении рисками цифровой безопасности и предполагает привлечение к обсуждению и выработке решений представителей компаний, работающих в сфере цифровой экономики.

В декабре 2019 г. Группа провела первые консультации со стейкхолдерами [44]. В результате, во-первых, был выявлен подход представителей цифровой экономики, заключающийся в том, что, действительно, их многочисленные инициативы, в том числе регуляторного характера [45–47], следует дополнить правовым регулированием кибербезопасности, в том числе на универсальном уровне. Во-вторых, в дискуссии о кибербезопасности на уровне данной Группы была привнесена тематика цифровой экономики, обсуждение проблемных вопросов которой, как правило, не затрагиваются в пространстве обсуждений, проводимых Группой межправительственных экспертов.

И, наконец, нельзя не отметить, что в формате ООН обсуждение проблематики международной информационной безопасности ведется в рамках широкого обсуждения глобальной проблематики «цифровизации» и развития цифровой экономики. Данные вопросы отнесены к компетенции Группы высокого состава по цифровому сотрудничеству, занимающейся вопросами международного сотрудничества в сфере развития и распространения цифровых технологий при одновременном учете необходимости обеспечения доверия и безопасности в цифровой среде посредством принятия соответствующего Глобального обязательства [48]. Причем все эти аспекты глубоко интегрированы в общую повестку ООН в сфере устойчивого развития и его технологического обеспечения.

Все сказанное доказывает обоснованность и перспективность междисциплинарного подхода к обеспечению международной информационной безопасности и формирует новый горизонт осмысления дальнейших направлений международно-правового сотрудничества в данной сфере. Важнейшим результатом такого сотрудничества должно выступить сокращение цифрового разрыва между государствами, составной частью которого является разрыв в уровне кибербезопасности, что предполагает содействие со стороны развитых стран в укреплении соответствующего потенциала развивающихся стран. Сюда следует отнести не только содействие укреплению кадрового потенциала развивающихся и наименее развитых государств, но и, как это предусмотрено, среди прочего, в п. 21 (c) Доклада группы межправительственных экспертов (раздел V международное сообщество и помощь в сфере обеспечения безопасности ИКТ и наращивания потенциала) за 2015 г., оказание помощи в обеспечении доступа к технологиям, которые имеют существенное значение для обеспечения безопасности ИКТ.

В настоящее время меры по оказанию помощи в сфере укрепления безопасности ИКТ-среды, как и меры по передаче и распространению ИКТ, имеют добровольный характер и предпринимаются на двухсторонней и многосторонней основе, в том числе в рамках международных организаций. Их следует рассматривать, например, в качестве составной части реализуемой в настоящее время инициативы по поддержке индустриализации Африки. И все же с учетом ключевой роли ИКТ для обеспечения перехода к устойчивому развитию, на наш взгляд, достаточно перспективным направлением международно-правового сотрудничества могли бы стать усилия по превращению международного информационного права, регулирующего в настоящее время информационный обмен, в отрасль международного права посредством разработки и принятия универсального кодифицирующего акта, предусматривающего международно-правовые обязательства как в сфере научно-технологического сотрудничества в сфере ИКТ, их передачи и распространения, так и оказания содействия развивающимся странам в повышении потенциала информационной безопасности с учетом строгих международно-правовых обязательств в сфере обеспечения глобальной информационной безопасности. В данном случае мог бы быть учрежден специальный международно-правовой режим, призванный стать надежной основой для реализации политических обязательств по развитию ИКТ-сектора и распространению цифровых технологий в Целях устойчивого развития. Одновременно это могло бы содействовать переходу к Индустрии-4.0 в условиях не усиления, а сокращения цифрового разрыва.

Подводя итоги проведенного исследования, необходимо сформулировать ряд выводов. Во-первых, логика цифровых трансформаций распространяется на осуществление МИНТС на все уровнях — универсальном, региональном и двустороннем, что вписывается в общий алгоритм Индустрии 4.0. Во-вторых, цифровые трансформации механизмов подобного рода сотрудничества актуализируют вопросы не только обеспечения технической безопасности разнообразных инфраструктур сотрудничества, включая различные платформы, использующие цифровые решения, но и достижение резистентности к киберугрозам. В-третьих, цифровые трансформации МИНТС в русле укрепления информационной безопасности инфраструктур и осуществляющегося на его основе взаимодействия являются важнейшим фактором, определяющим повышение вклада науки, технологий и инноваций в переход к устойчивому развитию и достижению его целей. В-четвертых, достаточно перспективным является развитие правовых основ, регулирующих сотрудничество не только государств, но и негосударственных акторов в сфере информационной безопасности международного научно-технологического сотрудничества и интеграции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Научный центр евразийской интеграции URL: https://eaisc.org/ (дата обращения: 15.08.2020).

2. Hoekman J., Frenken K., Tijssen R. J. Research collaboration at a distance. Changing spatial patterns of scientific collaboration within Europe // Research policy. 2010. Vol. 39. № 5. P. 662–673.

3. Трейссен Р. Научное сотрудничество и расширение научной сети: измерение процессов глобализации в мире // Международный форум по информации. 2012. Т. 37. № 2. С. 31–39.

4. Богданова И. Научные коммуникации в онлайновом пространстве // Наука и инновации. 2014. № 4. С. 12–16.

5. Болычев О. Н., Волошенко К. Ю. Межорганизационные сетевые взаимодействия как определяющая форма научно-технического и инновационного сотрудничества России и ЕС в Балтийском регионе // Балтийский регион. 2013. № 4. С. 23–39.

6. Костенко Н. И. Право международной информационной безопасности — новая отрасль международного публичного права // Кубанское агентство судебной информации Pro-Sud-123.ru: Юридический сетевой электронный научный журнал. 2018. № 1. С. 75–86.

7. Кузнецов П. У. Отдельные аспекты формирования правового обеспечения международной информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2016. № 4. С. 38–43.

8. Дальновидный подход к цифровому развитию. Доклад Генерального секретаря ООН, п. 65 // E/CN.16/2016/3 (29 февраля 2016 г.). URL: https://www.unctad.org/meetings/en/SessionalDocuments/ecn162016d3_ru.pdf (дата обращения: 05.07.2020).

9. The New Europe in the Global Digital Era. Current Rule-Market, Future Investor? I–Com Study, 04.11.2019. URL: https://www.i-com.it/en/2019/11/06/the-new-europe-in-the-global-digital-era-current-rule-maker-future-investor/ (дата обращения: 02.08.2020).

10. Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. 2019. № 3. С. 64–68.

11. Костенко Н. И. Право международной информационной безопасности (становление, тенденции и проблемы развития). — М. : Юрлитинформ, 2019. 464 с.

12. Капустин А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6. С. 44–51.

13. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности // Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря ООН // Док. ГА ООН A/70/174 (22 июля 2015 г.). URL: https://www.undocs.org/ru/A/70/174 (дата обращения: 14.08.2020).

14. Данагская декларация 25-й встречи лидеров экономик АТЭС (11 ноября 2017 г.) «С новой динамикой — к общему будущему». П. 13 «Подготовка качественных людских ресурсов для цифровой эпохи». URL: http://kremlin.ru/supplement/5253 (дата обращения: 19.07.2020).