УДК 341.018:327.7:004.77

ИСТОЧНИКИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОНЛАЙН-ПРОСТРАНСТВА В РАМКАХ ООН

Е.Ф. Ивашкевич
ВГУ имени П.М. Машерова, Республика Беларусь

Аннотация. В статье дана краткая характеристика актуальных проблем в области правового обеспечения киберзащищённости личности, общества и государства, основного содержания международных документов ООН, посвящённых их эффективному разрешению.

Ключевые слова: онлайн-пространство, онлайн-угрозы, кибербезопасность.

Последние десятилетия отмечены активной правотворческой деятельностью международного уровня в ответ на стремительное развитие интернет-отношений, становление их исключительного многообразия, превращение онлайн-пространства в одну из ключевых сфер жизни современного человека. Согласно данным специализированного учреждения ООН Международного союза электросвязи, в конце 2019 г. на планете насчитывалось 4 млрд. интернет-пользователей, что составило 51% от мирового населения [1], и данный показатель увеличился вдвое по сравнению с 2010 г. (2 млрд. человек). При этом Генеральный директор ЮНЕСКО О. Азуле на заседаниях Комиссии по широкополосной связи в 2019 г. подчеркнула роль цифрового доступа и цифровой грамотности в достижении целей устойчивого развития. В перспективе в рамках деятельности специализированных структур ООН планируется продвигать концепцию «значимого всеобщего подключения» и постоянно увеличивать процент домохозяйств, имеющих доступ к интернету, который на конец 2019 г. составил 54.8% [2]. Цель данной статьи – раскрыть основные направления правотворчества ООН в сфере регулирования киберпространства на современном этапе.

Материал и методы. Основным материалом для данного исследования послужили международные правовые акты ООН в области интернет-отношений. В работе использованы формально-юридический и структурно-аналитический методы исследования.

Результаты и их обсуждение. Очевидная недостаточность и неэффективность односторонних действий государств в обеспечении стабильной кибербезопасности возлагает серьезную ответственность на международное сообщество за формирование единых комплексных систем противостояния онлайн-угрозам. Ведущей организацией в сфере содействия созданию единообразного подхода к актуальным проблемам современности по праву является ООН, которая неоднократно признавала острую необходимость скорого решения ключевых проблем недостаточного урегулирования сети интернет.

В 2003 г. ГА ООН приняла Резолюцию «Создание глобальной культуры кибербезопасности», которая одной из первых обратила внимание на существование самого понятия «кибербезопасность» и выработала ряд неизбежных составляющих ее достижения. Формирование онлайн-сообщества невозможно отрицать, его влияние на все сферы жизни современного общества с каждым годом становится все сильнее, в связи с чем Резолюция предлагает поставить це-

лью достижение состояния наибольшей защищенности человека и общества от кибер-угроз. В документе подчеркивается, что кибербезопасность невозможно достигнуть индивидуально, она не является проблемой одного государства и его правительства, в данной области должно оказываться повсеместное сотрудничество. ГА ООН выработала 9 взаимодополняющих элементов достижения кибербезопасности: осведомленность, ответственность, реагирование, этика, демократия, оценка риска, проектирование и внедрение средств безопасности, управление обеспечением безопасности, переоценка. В раскрытии приведенных элементов Резолюция видит непосредственную инструкцию взаимодействия государств и других участников онлайн-отношений [3].

В этом же году была принята Рекомендация ООН о развитии и использовании многоязычия и всеобщем доступе к киберпространству, подчеркнувшая особую роль ООН в области информации и коммуникации. Документ был издан с целью призвать государства-члены и международные организации признать и оказывать поддержку всеобщему доступу к интернету в качестве одного из средств содействия осуществлению прав человека, указанных в ст. 19 и 27 Всеобщей декларации прав человека, посредством соответствующей политики в целях расширения прав граждан и развития гражданского общества, а также путем содействия и ее поддержки в развивающихся странах с должным учетом потребностей населения особенно в сельской местности. В качестве способа обеспечения всеобщего доступа к киберпространству было выдвинуто предложение по созданию на местном национальном, региональном и международном уровнях содействующих ему механизмов, причем расходы, связанные с использованием телекоммуникаций и интернета, должны быть доступными, а особое внимание должно уделяться потребностям общественных служб и учебных заведений, а также неимущих или обездоленных групп населения. Для этого Рекомендация предлагает разработать меры по стимулированию инвестиций в данную область, включая новые формы партнерства между государственным и частным секторами и уменьшение препятствий финансового характера на пути использования ИКТ, таких, как налоги и таможенные пошлины на компьютерное оборудование, программное обеспечение и услуги [4].

Стоит отметить, что ООН как участник онлайн-пространства сама неоднократно становилась жертвой недостаточной киберзащищенности. В 2013 г. был предоставлен Доклад Генсека ООН, в котором был выработан оперативный план действий по устранению замечаний в данной сфере по результатам деятельности Комиссии ревизоров по вопросам уязвимости информационных систем Секретариата ООН. Проблемы, отмеченные в Докладе, являются повсеместно распространенными. В первую очередь, в Докладе уделялось особое внимание техническому оснащению и обеспечению систематического мониторинга со стороны приглашённых экспертов соответствующей специализации, усилению превентивных мер контроля, проверке всех пакетов ПО, своевременному выявлению попыток несанкционированного доступа, установке систем оценки степени защищенности. Непосредственно столкнувшись с проблемой

кибербезопасноти, ООН активно предлагает наиболее эффективные способы реагирования на кибер-атаки [5].

В 2015 г. Экономический и социальный Комитет ООН по Западной Азии представил Политические рекомендации по кибербезопасности и борьбе с киберпреступностью в Арабском регионе. В исследовании приводится аналитический обзор текущей ситуации с киберпреступностью и кибербезопасностью на региональном и международном уровнях и освещаются меры по укреплению и согласованию усилий по борьбе с киберпреступностью, предлагаются руководящие правовые рамки для повышения кибербезопасности и доверия к информационно-коммуникационным технологиям и киберпространству. Документ подчеркивает необходимость закрепления нормативных и процедурных рамок для борьбы с кибер-угрозами и повышения осведомленности отдельных лиц и учреждений о таких рисках и их влиянии на работу и личную жизнь [6].

В 2020 г. в связи с тем, что автомобильный сектор переживает глубокую трансформацию и цифровизацию, которые необходимы для обеспечения автоматизации транспортных средств, возможности подключения и совместной мобильности, ООН издало Правила по кибербезопасности и обновлениям программного обеспечения. В документе отмечается, что стремительное увеличение количества «умных» автомобилей сопряжено со значительными рисками кибербезопасности, поскольку хакеры стремятся получить доступ к электронным системам и данным, угрожая безопасности транспортных средств и конфиденциальности пользователей. Правила ООН о кибербезопасности и обновлениях ПО призваны помочь справиться с этими рисками путем установления четких требований к производительности и аудиту автомобилей. Правила ООН 2020 г. являются первыми согласованными обязательными нормами в данной области на международном уровне [7].

ООН продолжает активно развивать международное правотворчество в области регулирования автоматизированных транспортных средств. На данный момент последним документом, принятым ООН в области правового регулирования киберпространства на международном уровне, являются Правила ООН № 155 «Кибербезопасность и управление системами кибербезопасностью», который во многом дополняет Правила ООН 2020 в ранее неурегулированной области. Новые правила выходят далеко за рамки существующих требований в отношении кибербезопасности в транспортных средствах. Под надзором компетентных органов производители соответствующих транспортных средств должны будут обеспечить, например, следующее:

– создание и наличие системы управления кибербезопасностью транспортных средств в дорожном движении;
– проведение анализа рисков кибербезопасности;
– механизмы снижения выявленных киберрисков;
– документация о функционирующих механизмах управления рисками;
– меры по выявлению и предотвращению кибератак;
– меры по поддержке ИТ-криминалистики в случае кибератак;

– постоянный мониторинг конкретных типов инцидентов кибербезопасности;

– сообщение об инцидентах кибербезопасности в компетентный орган по разрешению.

Очевидно, новые правила ООН свидетельствуют том, что сфера автомобильной кибербезопасности будет все активнее регулироваться. Целью этих правил является предотвращение ситуаций прогрессирующей оцифровки транспортных средств путем атак, как, например, это происходит с устройствами с доступом к интернету, посредством которых злоумышленники изобретают новые способы совершения преступлений в обход существующей системы ИТ-безопасности. Однако для соблюдения данных правил производители автомобилей и их поставщики должны будут приложить огромные усилия для соответствия всем требованиям, в связи с чем необходимо как можно быстрее начать массовую реализацию стратегии защиты от кибер-рисков [8].

Несмотря на то, что принятие ООН подобных правил является чрезвычайно важным для утверждения состояния всеобщей кибербезопасности как отдельных государств, так и международного сообщества в целом, данные документы в области автоматизированных ТС являются узкоспециализированными и, к сожалению, неприменимы к другим областям, которые остаются уязвимыми перед кибер-угрозами.

Следующим шагом на пути к достижению кибербезопасности стала разработка проекта Конвенции об обеспечении международной информационной безопасности. Целью Конвенции является противодействие использованию информационно-коммуникационных технологий для нарушения международного мира и безопасности. Основной акцент делается непосредственно на информационную безопасность, составной частью которой является кибербезопасность, что отрицательно сказывается на обеспечении наиболее полного регулирования именно интернет-среды. Проект документа предусматривает обязательство государств сотрудничать между собой в ходе формирования системы международной информационной безопасности, руководствуясь принципами неделимости безопасности и ответственности за собственное информационное пространство. Агрессивная «информационная война» признается преступлением против международного мира и безопасности [9].

Помимо непосредственного регулирования киберпространства с помощью специальных НПА, в рамках ООН действует группа правительственных экспертов по кибербезопасности. Ряд подразделений, сфера деятельности которых пересекается с онлайн-пространством, также занимается некоторыми вопросами обеспечения кибербезопасности, к таким платформам можно отнести ITU, UNIDIR, CTITF WorkingGroup, UNODC, UNICRI.

Заключение. Таким образом, компетентные органы ООН стараются оперативно реагировать на возникающие правовые пробелы в области кибер-законодательства, однако предлагаемые решения часто являются точечными и локальными. К сожалению, на данный момент не существует основополагающего международного акта, который обозначил бы проблемы и заложил прин-

ципы обеспечения кибербезопасности. Возможно, именно ООН стоит разработать подобный документ с целью недопущения возникновения дальнейших правовых коллизий в области оперативного реагирования на кибер-угрозы как на международном, так и локальном уровнях. Назрела необходимость закрепления на международном уровне перечня вопросов, непосредственно относящихся к базису состояния киберзащищенности, определения и классифицирования видов и уровней киберагресии.

Список использованных источников

1. International Telecommunication Union Statistics [Electronic resource]. – Mode of access: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. – Date of access: 29.04.2023.
2. ОфициальныйсайтUNESCO [Electronic resource]. – Mode of access:https://ru.unesco.org/news/v-novom-doklade-o-sostoyanii-shirokopolosnoy-svyazi-podcherkivaetsya-nastoyatelnaya.– Date of access: 07.05.2023.
3. Резолюция «Создание глобальной культуры кибербезопасности» № 57/239: принята ГА ООН, 31.01.2003 г. [Электронный ресурс]. – Режим доступа: https://undocs.org/ru/A/RES/57/239. – Дата доступа: 01.05.2023.
4. Рекомендация ООН о развитии и использовании многоязычия и всеобщем доступе к киберпространству от 15 октября 2003 г. [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml. – Дата доступа: 03.05.2023.
5. Доклад ГА ООН «Деятельность по осуществлению рекомендаций, касающихся укрепления информационной и системной безопасности во всех подразделениях Секретариата» от 20.03.2009 г. [Электронный ресурс]. – Режим доступа: https://undocs.org/ru/A/68/552. – Дата доступа: 30.04.2023.
6. Policy Recommendations on Cyber safety and Combating Cybercrime in the Arab Region: Summary [Electronic resource]. – Mode of access: https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf. – Date of access: 02.05.2023.
7. UN Regulations on Cybersecurity and Software Updates 2020 [Electronic resource]. – Mode of access: https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf. – Date of access: 03.05.2023.
8. UN Regulation No. 155. – Cyber security and cyber security management system 2021 [Electronic resource]. – Mode of access: https://unece.org/transport/documents/-2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. – Date of access: 03.03.2021.
9. Draft Conventionon International Information Security [Electronic resource]. – Mode of access: https://www.pircenter.org/kosdata/page_ doc/p2728_1.pdf. – Date of access: 06.05.2023.
10. Ивашкевич, Е.Ф. Государственная правовая политика в сфере регулирования онлайн-пространства в Республике Беларусь и зарубежных странах / Е.Ф. Ивашкевич, П. Смирнов // Юридическое образование в Республике Беларусь и зарубежных странах: сб. науч. статей [по итогам науч.-практ. конф., Витебск, 2-3 ноября, 2018 г.]. – Витебск: ВГУ имени П. М. Машерова, 2018. – С.192-199. URL: https://rep.vsu.by/handle/123456789/17233 (дата обращения: 07.05.2023).