УДК 341.1/8

СТАНОВЛЕНИЕ ИДЕИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРОГНОЗЫ НА БЛИЖАЙШЕЕ БУДУЩЕЕ

Е. В. Калинина
Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского

Эпоха глобализации, сопровождающаяся интенсивным научно–техническим прогрессом, вынесла на «повестку дня» проблему международной информационной безопасности. В отличие от западных государств, сфокусировавших внимание на разработке отдельных, узкоспециализированных аспектов, таких как кибертерроризм, киберпреступность, Россия пытается добиться комплексного решения вопроса об ответственном использовании информационных технологий и информационного пространства.

Ключевые слова: международная информационная безопасность, кибербезопасность, киберпространство, международное сотрудничество.

Е. В. Калинина
Профессор кафедры европейского и международного права юридического факультета Национального исследовательского Нижегородского государственного университета им. Н.И. Лобачевского, доктор юридических наук, доцент

Процессы, происходящие в мире и являющиеся «побочными эффектами» глобализации, в немалой степени способствуют приданию ряду вызовов национальной безопасности транснационального характера. К таким аспектам относится информационная безопасность.

Последние десятилетия ситуация осложнялась не только неспособностью государств прийти к универсальному компромиссу в выборе средств реагирования на информационные угрозы коллективной безопасности и предоставлении доступа к важным данным, что может рассматриваться как посягательство на идею государственной юрисдикции и государственного суверенитета, но и весьма банальным непризнанием самой проблемы информационной безопасности.

Обсуждение данной проблематики, в т.ч. на международных конференциях, на «площадках» разного уровня, включая ООН, ШОС, ОДКБ и прочие, показало, что многие ученые и практики не в полной мере осознавали потенциал рисков и вызовов, связанных с применением инструментария «мягкой силы» интерактивного поколения. Научный и политический мир только сейчас начал «бить тревогу» по поводу вполне очевидных опасностей и угроз, хотя специалисты предупреждали общественность с начала первых атак на автоматизированные системы.

Понятия «информационная безопасность», «кибербезопасность», «кибертерроризм», «киберпре–

ступления» прочно вошли в нашу жизнь. Зачастую первые два используются как идентичные категории. Тем не менее в российской практике, согласно мнению большинства исследователей, чаще применяется формулировка «информационная безопасность», а в западной – «кибербезопасность».

Мы не можем согласиться с эквивалентностью данных понятий, полагая, что конструкция «информационная безопасность» содержательно шире «кибербезопасности». Последнюю целесообразно рассматривать в качестве раздела информационной безопасности, предметом которого являются процессы формирования, функционирования и защиты вычислительных устройств, в то время как «информационная безопасность» является универсальным понятием, предполагающим состояние защищенности информации, данных (независимо от их формы – электронной или физической) от несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения.

Защита информации и защита компьютерной инфраструктуры от разрушения и сбоев различаются по целям и задачам. В первом случае речь идет о недопущении утечки информации; во втором сохранение информации отходит на второй план, поскольку основная цель – бесперебойная работа автоматизированных систем.

В современной науке, нормативных актах международного и национального уровня и практической деятельности не было признано унифицированного подхода к определению искомого концепта, что создает сложности при выработке пути сопротивления вызовам, возникающим в информационном пространстве.

А.В. Кубышкин предлагает следующее определение понятия «информационная безопасность»: это «состояние защищенности личности, общества, государства от информации, носящей вредный или противоправный характер, от информации, оказывающей негативное влияние на сознание личности; препятствующей устойчивому развитию личности, общества и государства»[1].

Однако категория информационной безопасности имеет комплексный объект, поэтому ученый добавляет, что ИБ – это также «обеспечивающее устойчивое развитие состояние защищенности информационной инфраструктуры, включая компьютеры и информационно–телекоммуникационную инфраструктуру, и информации, в них находящейся»[2].

Для целей настоящего исследования, анализируя концепт международной информационной безопасности, мы будем исходить из расширительного его понимания: международная информационная безопасность – это одновременно 1) и состояние защищенности субъектов международного права (МП) от информации, носящей вредный или противоправный характер, а также оказывающей негативное воздействие на сознание населения; 2) и состояние защищенности информационной инфраструктуры субъектов МП; 3) и система организационно–правовых средств, обеспечивающая защиту сетей, компьютеров, программ, устройств от атак, повреждения или несанкционированного доступа, призванная обеспечить эффективное сотрудничество акторов в международном информационном пространстве.

История становления идеи международной информационной безопасности (МИБ). Можно было бы последовать примеру ряда авторов, «погружающихся» в глубь веков и анализирующих историю защиты информации, начиная с весьма примитивных ее, защиты, видов, до сложных криптографических конструкций.

Представляется, однако, предпочтительным анализ непосредственной истории идеи информационной безопасности, т.е. в ее современном понимании.

Становление концепта МИБ совпадает с эволюцией международно–правового регулирования информационных отношений в Новейшее время. В этой связи весьма интересной выглядит периодизация, предложенная в одной из первых диссертаций, посвященных праву МИБ, выполненной исследователем А.В. Кубышкиным. Ученый выделяет 3 этапа: «1–й этап – появление международно–правового регулирования аспекта информационных отношений, связанного с содержанием информации»; «2–й этап – разработка концепции нового международного информационного порядка»; «3–й этап – развитие международно–правового регулирования в области обмена информацией в связи с увеличением масштабов непосредственного телевизионного вещания через космические спутники»[3].

Несмотря на очевидную логику подобного подхода, нельзя не обратить внимание на существенный недочет: первый и второй этапы, что также следует из рассуждений автора, имеют одну и ту же цель и характеризуются тем же предметом правового регулирования (содержание информации).

Кроме того, с 90–х годов XX века наблюдается усложнение международных информационных от–

ношений, вызванное вынужденным признанием не только удобств развития компьютерных технологий, но и риска «побочных эффектов». Это усложнение вызывает к жизни категорию «кибербезопасности», т.е. ученые и практики от политики и юриспруденции, не говоря уже о технических специалистах, начинают рассуждать о защите от атак сетей, компьютеров, программ и устройств.

В свете вышесказанного, целесообразнее было бы обозначить исследуемые временные рамки: с начала XX века – до наших дней. В свою очередь, этот временной отрезок поддается делению на 2 периода: 1) 1923–1989 гг. – формирование нормативно-правовой базы регулирования международных информационных отношений и разработка концепции нового международного информационного порядка; 2) с 1989 г. по наше время – начало истории кибербезопасности; переплетение категорий «информационная безопасность» и «кибербезопасность».

На ранних стадиях развития компьютерных сетей проблема их безопасности не обсуждалась по причине ограниченного и немногочисленного круга пользователей и их локальности. Интенсивное развитие технологий и расширение сетей связи заставили задуматься об обеспечении безопасности автоматизированных систем. Поэтому в последнее время понятие «кибербезопасность» используется наряду с термином «информационная безопасность». Принято считать, что точкой отсчета истории кибербезопасности являтся осуществление первых атак на компьютеры (например, первый компьютерный червь, созданный Робертом Моррисом в 1989 г.).

В настоящее время кибербезопасность становится одной из наиболее дискуссионных тем, что объясняется широким использованием компьютерных технологий не только в профессиональной деятельности, но и в обыденной жизни.

Россия является одним из наиболее активных участников переговорного процесса в поисках оптимального взаимодействия в целях обеспечения коллективной информационной безопасности. Предложения российской стороны о создании правил добросовестного поведения государств в информационном пространстве неоднократно принимались к рассмотрению на Генеральной Ассамблее ООН. К сожалению, политическое соперничество основных акторов международных отношений до сих пор препятствует достижению компромисса. Тем не менее представленный 5 декабря 2018 г. на голосование Проект резолюции ГА ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», содержащий правила ответственного поведения государств в киберпространстве, был поддержан подавляющим большинством участников.

А. Бедрицкий, анализируя опыт российских инициатив и реакций на них со стороны ведущих держав и их сторонников, выделяет 2 следующих основных подхода к проблеме информационной безопасности.

1) США и Европа сосредоточили свое внимание на отдельных проблемах международной информационной безопасности, выбрав в качестве приоритетного направления противодействие угрозам террористического и криминального характера, что привело к созданию на европейском уровне конвенции о борьбе с преступлениями в киберпространстве. Вопрос разоружения серьезно не рассматривался, ввиду скептического отношения к идее «информационного оружия» и «информационной войны» в целом.

2) Иной путь выбрали для себя Россия, ее партнеры по ШОС и представители развивающихся стран, настаивающие на комплексном анализе проблемы международной информационной безопасности, определяя в качестве основной цели предотвращение опасности развязывания информационной войны[4]. Они также настаивали на назревшей необходимости разработки международно-правовой основы универсального режима МИБ[5].

В ближайшем будущем ожидается сохранение следующих тенденций. 1) Национальные интересы государств и искусственно подпитываемое взаимное недоверие будут продолжать препятствовать достижению компромисса по противодействию информационным угрозам. Это будет обусловливать склонность государств к защите собственной инфраструктуры без качественных изменений в переговорных механизмах. Осознавая необходимость международного сотрудничества по обеспечению коллективной безопасности, в условиях противостояния с Западом, Россия продолжит активные мероприятия на региональном уровне.

2) На глобальном уровне будет сохраняться и усиливаться интерес в отношении нейтрализации киберпреступности, кибершпионажа, угроз финансовой и экономической устойчивости.

3) Все так же будет ощущаться недостаток квалифицированных специалистов, способных не только осуществлять организационно-правовое сопровождение защиты информации, но и активно участво-

вать в разработке международно–правовых норм информационной безопасности.

Пути преодоления современных вызовов МИБ. Во–первых, следует укреплять транснациональное сотрудничество. Развитие информационных технологий снимает ограничители в виде времени и расстояния, ускоряет процессы глобализации, делает прозрачными государственные границы, уничтожает экономические и социальные барьеры, объединяя территории государств в единое информационное пространство. Становятся очевидными недостаточность индивидуальной защиты национальных интересов в этом пространстве и необходимость межгосударственного сотрудничества в противодействии информационным угрозам.

Международное сотрудничество в сфере обеспечения информационной безопасности должно развиваться по следующим направлениям: разработка приемлемых для всех участников международного сообщества унифицированных технических и правовых норм, стандартов и инструкций по совместной защите информации (региональный и глобальный уровень); доработка мер по укреплению доверия; совместные научные исследования по созданию средств защиты информации; обмен опытом ведущих специалистов.

Во–вторых, необходимо создание и функционирование специализированных аналитических центров, оснащенных новейшими ИКТ, в штат которых следует ввести специалистов разного профиля: в сфере компьютерных технологий, политологов, юристов и психологов.

В–третьих, внедрение искомой проблематики в учебный процесс. В этой связи следует отметить, что в организации учебного процесса в современных российских вузах все не так уж безнадежно: 1) в подразделениях, вырабатывающих компетенции в сфере высшей математики и кибернетики, преподаются дисциплины, имеющие своим предметом информационную безопасность; 2) в рамках таких направлений подготовки, как правовое регулирование национальной безопасности, документоведение и архивоведение, создана специальная дисциплина по информационной безопасности; 3) на юридических факультетах читаются курсы информационных технологий в юридической деятельности, отдельными разделами которых является информационная безопасность.

Таким образом, нельзя сказать, что мы не идем в ногу со временем. Тем не менее все эти и аналогичные учебные дисциплины направлены на исследование национальной, государственной информационной безопасности, а в современном мире вопрос защиты данных уже давно переместился в разряд транснациональных.

В связи с этим выявилась проблема недостатка предложений образовательных продуктов по *праву международной информационной безопасности* в российских вузах. Так, регулярный мониторинг наличия таких предложений позволяет выявить в лучшем случае одно в год. Зато предложений об участии в летних и зимних школах по данной проблематике в зарубежных учебных заведениях гораздо больше, что заставляет задуматься о целесообразности интернационализации высшего образования. Для этого потребуется создание совместных международных научных и образовательных проектов, предусматривающих подготовку и переподготовку кадров, способных, в дальнейшем, осуществлять организационно–правовую деятельность по защите информации, а также разработка (на базе такого партнерства) новых модулей и курсов междисциплинарного характера, призванных сформировать профессионалов нового типа, специализирующихся на юридическом сопровождении компьютерных технологий.

Библиографический список

1. Кубышкин А.В. Международно–правовые проблемы обеспечения информационной безопасности государств: Дис. ... канд. юр. наук. М., 2002. 193 с.

2. Бедрицкий А. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. ПЕРСПЕКТИВЫ: Фонд исторической перспективы [Электронный ресурс]. URL: http://www.perspektivy.info/print.php?ID=232592 (дата обращения: 10.04.2019).

3. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; под общ. ред. А.В. Федорова, В.Н. Цыгичко. М.: ПИР–Центр, 2001. 328 с.

[1] Кубышкин А.В. Международно–правовые проблемы обеспечения информационной безопасности государств: Дис. ... канд. юр. наук. М., 2002. С. 29.

[2] Там же.

[3] Там же. С. 31–39.

[4] Бедрицкий А. Международные договоренности по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. ПЕРСПЕКТИВЫ: Фонд исторической перспективы [Электронный ресурс]. URL: http://www.perspektivy.info/print.php?ID=232592 (дата обращения: 10.04.2019).

[5] См.: Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; под общ. ред. А.В. Федорова, В.Н. Цыгичко. М.: ПИР–Центр, 2001. С. 186–187.

DEVELOPING THE IDEA OF INTERNATIONAL INFORMATION SECURITY. FUTURE EXPECTATIONS

E. V. Kalinina

Professor of the Department of European and International Law of the Law Faculty of the Lobachevsky State University of Nizhny Novgorod, Doctor of Sciences (Law), Associate Professor

The era of globalization accompanied with its rapid rate of scientific and technological progress has put the problem of international information security on the agenda. Unlike foreign countries focusing their attention on particularized topics such as cyberterrorism and cybercrime, the Russian Federation endeavors to achieve a comprehensive solution to the issue of responsible use of information technologies and information space.

Keywords: international information security, cybersecurity, cyberspace, international cooperation.