Никонова Людмила Ивановна
доцент кафедры конституционного и международного права
Юридический институт НИУ «БелГУ»
кандидат юридических наук, доцент
Бондарева Алина Владимировна
студентка Юридического института НИУ «БелГУ»
(Белгород)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ТЕРМИНОЛОГИЧЕСКИЕ И СОДЕРЖАТЕЛЬНЫЕ РАЗЛИЧИЯ

«Все наиболее значимые результаты в праве и юридической науке достигались вследствие их методологической ориентации на объективную необходимость, определенность, устойчивость, обратимость, причинность, истинность, точность и другие качества знаний, превозносимые классической наукой»[1].

Актуальность вопросов международного сотрудничества государств в сфере информационной безопасности обусловлена зависимостью всех сфер жизни современного общества от информационных технологий[2]. Распространение новейших глобальных средств коммуникации, с одной стороны, открывает колоссальные возможности для развития общества, а с другой, порождает многочисленные проблемы, связанные с угрозами применения современных ИКТ, решение которых возможно только совместными усилиями международного сообщества.

Нормативное определение «международной информационной безопасности» содержится в п. 6 Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Под ней понимается «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры»[3].

---

[1] Мальцев Г.В. Социальные основания права. М., 2007. С. 101-102.

[2] Макогон Б.В. Современное государство в условиях глобализации // Пробелы в российском законодательстве. 2012. № 2. С. 29-31.

[3] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 № Пр-

Исходя из данной дефиниции, можно сделать вывод, что содержательная часть включает в себя как технические аспекты (критическую информационную инфраструктуру), так и обширный круг политико-идеологических моментов (манипулирование информацией, пропаганду посредством глобальных информационных сетей, информационное воздействие и др.).

Согласно ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1] критическая информационная инфраструктура включает как объекты (информационные системы, автоматизированные системы управления субъектов критической информационной инфраструктуры, информационно-телекоммуникационные сети), так и сети электросвязи, используемые для организации их взаимодействия. Например, информационные системы сети госорганов, автоматизированные системы управления технологическими процессами в оборонной индустрии, в сфере здравоохранения, связи, на транспорте, в кредитно-финансовой сфере и энергетике, а также в ряде отраслей промышленности, включая топливную, атомную, ракетно-космическую и другие отрасли.

Представители Центра стратегических оценок и прогнозов к критически важному сегменту информационной инфраструктуры России относят «такую информационно-телекоммуникационную систему, выход из строя или нарушение режима функционирования которой может оказать негативное влияние на состояние национальной безопасности Российской Федерации»[2]. В критически важный сегмент информационной инфраструктуры включены: системы телекоммуникаций военного и специального назначения; системы управлений энергетикой, транспортом, водными системами; ИТС служб реагирования на чрезвычайные ситуации; банковские и финансовые ИТС; другие государственные и частные ИТС, минимально необходимые для функционирования экономики и государства.

Второй составляющей в российской версии определения международной информационной безопасности является информационно-психологическая, под которой понимается «состояние защищенности от негативных информационно-психологических воздействий в связи с

1753) // Официальный сайт Совета Безопасности РФ; URL: http://www.scrf.gov.ru (дата обращения 05.04.2018).

[1] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 27.07.2017. (дата обращения 05.04.2018).

[2] Информационная война и защита информации. Словарь основных терминов и определений // Центр стратегических оценок и прогнозов. М., 2011. С. 32.

использованием специальных средств и методов воздействия на психику отдельных лиц и (или) групп лиц, и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере»[1].

По мнению Д.А. Молчанова, именно такая структура, сочетающая в себе как технические, так и психологические аспекты информационной безопасности характеризует выбор российской терминологии[2].

Для эффективного сотрудничества между странами в информационной сфере необходима однозначная интерпретация используемых понятий. Зарубежные страны, и прежде всего США, в отличие от России используют термин «cybersecurity». Данная формулировка применяется и Международным союзом электросвязи, членами которого является 191 государство. Кибербезопасность – это совокупность инструментов, политик, понятий безопасности, гарантий безопасности, рекомендаций, подходов управления рисками, действий, обучения, лучших практик, гарантий и технологий, которые используются с тем, чтобы защитить киберсреду («cyberspace») организации-пользователя и активы пользователя. Организация-пользователь и активы пользователя включают связанные вычислительные устройства, персонал, инфраструктуру, прикладные технологии, услуги, телекоммуникационные системы и совокупность переданной и/или сохраненной информации в киберсреде»[3].

В Международной стратегии США для киберпространства «Процветание, безопасность и открытость сетевого мира» 2011 г.[4] определение «cybersecurity» также отражает только один аспект, связанный со средствами обработки информации. Кибербезопасность представляет собой защиту и оборону информации и информационных систем против несанкционированного доступа или модификации информации, находящейся в процессе хранения, обработки или передачи, а также против прекращения функционирования системы для санкционированных пользователей.

---

[1] Баришполец В.А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. 2012. № 5. С. 65.

[2] Молчанов Д.А. Дифференциация содержания понятия «информационная безопасность» в национальном законодательстве Российской Федерации и Соединенных Штатов Америки как сдерживающий фактор прогрессивного развития международно-правового регулирования [Электронный ресурс] // Право: современные тенденции: материалы IV Междунар. науч. конф. (г. Краснодар, февраль 2017 г.). Краснодар: Новация, 2017. С. 122-125; URL: https://moluch.ru/conf/law/archive/225/11706/ (дата обращения 05.04.2018).

[3] Касенова М.Б. Трансграничное управление Интернетом: основные термины и понятия [Электронный ресурс] // Юридический мир. 2014. № 2. (206). С. 58-63.

[4] International Strategy For Cyberspace, Washington DC. Prosperity, Security, and Openness in a Networked World // The White House : offic. website. 2011. May.25 p. URL: http://www.white house.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения 05.04.2018).

Информационная безопасность включает меры, необходимые для обнаружения, документирования и ответа на эти угрозы[1].

О выявлении проблем семантического характера при использовании терминов пишет М.Б Касенова. Так, «cybersecurity» напрямую связана с «cyberspace». Термин «cyberspace» применятся в документах Международного союза электросвязи, где означает среду с подключенными компьютерными устройствами, пользователями, инфраструктурой, приложениями, сервисами, телекоммуникационными системами, а также совокупность передаваемой и (или) хранящейся в этой среде информации. В то же время в национальном законодательстве Польши данный термин имеет иное содержательное значение (пространство производства и обмена информацией, создаваемой телеинформационными системами)[2].

В России формулировка «киберпространство» не применяется, а используется «информационное пространство». Оно определено как «сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию»[3].

Смысловые и содержательные различия употребления тех или иных терминов зависят также и от вариантов их перевода на другие языки. Например, слово «cybersecurity» с английского языка на русский буквально переводится как «кибербезопасность», но Россия использует понятия «информационная безопасность» или «безопасность применения информационно-коммуникационных технологий». Следует отметить, что не только в России применяется данный термин. Например, он сформулирован и закреплён в концепции Конвенции об обеспечении международной информационной безопасности, предложенной к рассмотрению на 66-й сессии Генеральной Ассамблеи ООН в 2011 г. Китаем, Россией, Таджикистаном и Узбекистаном.

Согласно данной Конвенции «международная информационная безопасность» представляет собой состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы

---

[1] Касенова М.Б. Указ. соч. С. 60.

[2] Цит. по: Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном пространстве // Юридический мир. 2016. № 8. С. 63-66.

[3] Конвенция об обеспечении международной информационной безопасности (концепция) // Официальный сайт Министерства иностранных Дел Российской Федерации; URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29 (дата обращения 05.04.2018).

безопасности государств и мирового сообщества в информационном пространстве»[1].

Модельный закон стран Содружества Независимых Государств 2002 г. «О международном информационном обмене» также использует понятие информационная безопасность и определяет ее как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства»[2].

Концепция сотрудничества государств - участников СНГ в сфере обеспечения информационной безопасности, утвержденная Советом глав государств СНГ в 2008 г., трактует информационную безопасность как «состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства»[3]. Такой узкий технократический подход, включающий только ее защиту, существенно сужает проблему информационной безопасности. Поэтому в Рекомендациях предлагается использовать сущностную трактовку, закрепленную в тексте Соглашения между Правительствами государств - членов Шанхайской организации сотрудничества «О сотрудничестве в области обеспечения международной информационной безопасности» (Екатеринбург, 2009 г.). В этом документе анализируемая категория представлена как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[4]. Такая дефиниция включает в себя в том числе, и актуальные угрозы социально-гуманитарного плана, например, угрозу распространения информации, наносящей вред общественно-политической и социально-экономической системам государства, духовной, нравственной или культурной среде общества.

---

[1] Там же.

[2] Модельный закон «О международном информационном обмене» (Принят постановлением Межпарламентской Ассамблеи государств-участников СНГ от 26 марта 2002 г. № 19-7) // Информационный бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2002. № 29; URL: http://base.garant.ru/2569410/ (дата обращения 05.04.2018).

[3] Концепция сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и Комплексный план мероприятий по реализации Концепции сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности 2008 г. [Электронный ресурс] // Интернет портал стран СНГ;URL: http://www.e-cis.info/page.php?id=20229 (дата обращения 05.04.2018).

[4] Распоряжение Правительства РФ от 16 июля 2009 г. № 984-р «Об утверждении Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // Текст Распоряжения официально опубликован не был; URL:: http://www.garant.ru (дата обращения 05.04.2018).

В действующем сегодня Соглашении о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности от 2013 г. информационная безопасность понимается как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[1].

Таким, образом, для эффективного и плодотворного международного сотрудничества государств по созданию системы информационной безопасности странам необходимо прийти к консенсусу относительно использования идентичных дефиниций и содержания понятий в данной сфере. Так как западные страны (члены Международного союза электросвязи) и США используют термин «cybersecurity», а Россия и государства-участники региональных организаций СНГ и ШОС – «информационная безопасность». Разницу в формулировках сопровождает и разное наполнение содержательной сущности данных терминов. Так, Россия придерживается широкого подхода к определению структуры информационной безопасности и включает в нее как информационно-техническую сферу, так и информационно-психологическую (психофизическую) составляющую. Западные страны и США придерживаются более узкого подхода, ограничиваясь только технической сферой.

Нифанов Алексей Николаевич
доцент кафедры конституционного и международного права
Юридический институт НИУ «БелГУ»
кандидат юридических наук, доцент
(Белгород)

ТЕОРЕТИКО-ПРАВОВЫЕ ПРОБЛЕМЫ ПРИГРАНИЧНОЙ ТЕРРИТОРИИ В КОНТЕКСТЕ КОНСТИТУЦИОННОГО ПРАВА

«Мир, действительно, во многом не определен, но право должно добиваться определенности, четкости отношений так, где это необходимо и важно для общества»[2].

---

[1] Распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р «О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности // Собрание законодательства РФ. 2013. № 47. Ст. 6135.

[2] Мальцев Г.В. Социальные снования права. М., 2007. С. 115.