Секция «Компьютерное право и информационная безопасность»

Теория киберсуверенитета, суверенитет и верховенство права в киберпространстве

Научный руководитель – Сомик Кирилл Васильевич

Кравченко Влада Игоревна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Москва, Россия
E-mail: vlada.kravchenko.2000@mail.ru

Под область традиционного суверенитета подпадают главным образом морские, наземные и воздушные территории. Прогресс кибертехнологий создал беспрецедентно новую форму общественного порядка. Так, киберпространство, будучи ранее неизвестной областью, невидимо, но при этом совершенно объективно существует в нашей реальной жизни. Первоначально границ в мире киберпространства не существовало, но очевидно, что киберпространство не может существовать в отрыве от стран, и именно поэтому, когда проблемы безопасности киберпространства стали угрожать государственной безопасности, в нем появились относительные суверенные границы. Научно-техническое развитие и общественные преобразования обусловили появление концепции киберсувернитета. Как было отмечено выше, в отличие от традиционного суверенитета, киберсуверенитет выделяет абсолютно «новые пространства» - новую территорию, которая существенно отличается от водных, земельных и воздушных владений. Однако важно отметить, что киберсуверенитет не возвышается над традиционном суверенитетом, а напротив, проистекает из теории традиционного суверенитета, принципов международного верховенства права [2]. Его появление было обусловлено необходимостью ограничить гегемонию в киберпространстве, поэтому киберсуверенитет, как и традиционный суверенитет, выполняют одну общую миссию - защиту государственной безопасности. В каком-то смысле киберсуверенитет это новое оружие традиционного суверенитета, появление которого в современных условиях было вызвано острой необходимостью [3].

Суверенитет в киберпространстве - еще одна принципиально новая идея. До ее появления платформенная часть сети был отнесена к верховенству телекоммуникационного права, объектная часть сети - к праву интеллектуальной собственности, субъекты и деятельность в сети - в основном регулировались нормами гражданского и уголовного права. Но с тех пор, как стало известно о том, какое непосредственное воздействие оказывает безопасность в киберпространстве на национальную безопасность, стало очевидно, что киберпорядок должен быть урегулирован с высоты суверенного верховенства права. Законодательно закрепленное определение киберпространства в разных странах неодинаково. Так, в Указе Президента США №54 "О национальной безопасности" под киберпространством понимают сеть, от которой зависит всякая ИТ-инфраструктура, включающая интернет, различные телекоммуникационные сети, различные компьютерные системы, встроенные процессоры и контроллеры в различных ключевых промышленных объектах. В то же время в Белой книге по обороне и национальной безопасности Франции дается другое определение, в соответствии с которым под киберпространством понимается пространство, состоящее из всех сетей, принципиально отличающееся от физического пространства, поскольку оно не имеет границ. В стратегии правительства Великобритании в области кибербезопасности 2009 г. не дают определения киберпространства, ограничиваясь перечислением элементов, его составляющих, так как все виды сетевых и цифровых действий, контент и

действия, осуществляемые через цифровые сети. Международная основа суверенитета в киберпространстве изложена в статье 20 «Доклада группы правительственных экспертов по развитию сферы информации и электросвязи с точки зрения международной безопасности», которая гласит, что «суверенитет государств и международные нормы и принципы, вытекающие из суверенитета, применяются к деятельности государств в отношении инфраструктуры ИКТ на их территории.

Законы и нормативные акты, принятые странами в области интернета, можно классифицировать по нескольким аспектам. Первое. Законы, регламентирующие управление информацией, угрожающей национальной безопасности, связанной с терроризмом и расовой дискриминацией. Например, Закон США «О патриотах» 2001 г., Закон РФ «О средствах массовой информации» 1991 г., Закон Германии «О защите прав в интернете» 2017 г., закон Сингапура «О практике использования интернета» 1991 г. Второй аспект-управление поведением в интернете. В качестве примера можно привести закон Сингапура «О поведении в интернете» 1996 г., или Закон Франции «Об информационном обществе» 2006 г. Третий аспект - управление информацией, угрожающей физическому и психическому здоровью детей, включая порнографию, насилие. В частности, это ФЗ РФ «О защите детей от информации, причиняющей вред их здоровью и развитию» 2010 г., Закон США «О защите детей в интернете» 2001 г., Закон Японии «Об исправлении условий, обеспечивающих безопасность молодежи в интернете» 2008 г. Четвертый аспект связан с борьбой со спамом: Закон США «О борьбе со спамом» 2003 г., ФЗ РФ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации". Пятый касается запрета на азартные игры в интернете: например, Закон Австралии «Об интерактивных азартных играх» 2001 г., а шестой направлен на защиту конфиденциальности. Например, закон Японии «О защите личной информации» 2003 г.

Стоит отметить, что США являются первой страной в мире сформулировавшей стратегию безопасности в киберпространстве. В 2003 г. Соединенные Штаты выпустили «Стратегию национальной безопасности в киберпространстве», которая включала требование, чтобы федеральное правительство, местные органы власти, частный сектор и граждане США сотрудничали в борьбе с угрозами киберпространства. Далее в мае 2011 г. США объявили о «Международной стратегии в киберпространстве», подчеркивающей важность безопасности в киберпространстве в дипломатических и экономических вопросах. В ноябре 2011 г. в закон США «О разрешении на оборону» был включен принцип, в соответствии с которым США имеют право на ответные действия в случае крупной кибератаки [1].

В России была сформирована правовая система национальной безопасности, включающая Конституцию РФ, ФЗ «О безопасности» 2014 г., Указ Президента «О Стратегии национальной безопасности Российской Федерации» 2015 г. Российская сторона придерживается позиции по достижению Международной конвенции о кибербезопасности. Международный союз электросвязи в рамках ООН работает над продвижением международного Договора о глобальном управлении в киберпространстве. В июле 2010 года 15 государств-членов ООН, в том числе Россия и США, подписали проект договора, направленного на снижение рисков киберпространства, в котором говорится о рекомендации ООН разработать кодекс поведения в киберпространстве.

Важно отметить, что поскольку сети взаимосвязаны, национальные законодательные тенденции в каждом государстве являются опытом и основой для будущего построения мирового порядка в киберпространстве.

Источники и литература

1) Лю Фэн, Линь Дундай. Система безопасности в киберпространстве США. Наука и образование, 2015. С. 39.

2) Сингер П.В., Фридман А. Кибербезопасность: проигрышная интернет война-война. Electronic Industry Press, 2015. С. 18.

3) Фан Биньсин. О суверенитете и кибербезопасности. Science Press, 2017. С.125.