Уголовно-правовая защита обеспечения информационной безопасности в зарубежных странах

Альханов Насрудин Магомедович
ст. преподаватель кафедры уголовного права и криминологии
ФГБОУ ВО "Чеченский государственный университет"

Учитывая, что в международном праве до сих пор не удалось создать единого подхода к определению информационной безопасности, в работе рассматриваются две полярные концепции относительно регулирования общественных отношений, касающихся проблем информационной безопасности. Сторонники первой концепции, которой придерживается и Россия, базируют свою позицию на широком понимании проблематики международной информационной безопасности. В её основу положены принципы неделимости безопасности и ответственности государств за своё информационное пространство. Согласно такому пониманию решения вопросов, касающихся поддержания информационной безопасности, противодействие угрозам военного (военно-политического), террористического и криминального характера использованием ИКТ, должно осуществляться системно. Соответственно, международно-правовое регулирование должно быть распространено на все указанные структурные элементы, и ради достижения этого предложено принятие международного соглашения на универсальном уровне.[1]

В рамках данной концепции особое место уделяется вопросу регулирования структурных элементов международной информационной безопасности. В связи с этим работе рассмотрены два основных направления международно-правового регулирования использования ИКТ: информационный («содержательный») коммуникационный («технический»), которые в доктрине определяются как функциональные. В международно-правовой проблематике информационной безопасности данные элементы рассматриваются позиций противодействия использования ИКТ, направленного на вред основным правам и свободам человека и крити чески важным структурам государств . В случае с информационным («содержательным») направлением — это противодействие трансграничному распространению посредством ИКТ информации, что противоречит принципам и нормам международного права, разжигает межнациональную, межрасовую и межконфессиональную вражду, распространяет расистские, ксенофобские письменные материалы, изображения или любую демонстрацию идей или теорий, которые пропагандируют, подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц . В случае с коммуникационным («техническим») направлением — это противодействие использованию коммуникационных систем, процессов и ресурсов против коммуникационных сетей и критически важных структур других государств, что наносит ущерб функционированию финансовой, политической, экономической и социальной системам.[2]

В целом, можно утверждать, что информационная безопасность в её международно-правовых основах представляет собой широкий перечень документов, который является основой для конструирований аналогичного понятия российской национальной доктрине информационной безопасности, а также для её понимания в уголовно-правовом смысле.

Основываясь на проведённом анализе международных документов и научной литературе, которая касается комплекса вопросов информационной безопасности человека, учреждения, общества государств , мы можем рекомендовать включить в будущий международный нормативный акт в сфере информационной безопасности (создание которого предусмотрено многочисленными Резолюциями ГА ООН) такие виды международной информационной безопасности, как глобальная

информационная безопасность (т.е. безопасность международного сообщества); информационная безопасность отдельных государств в международном информационном пространстве; информационная безопасность учреждений в международном информационном пространстве; информационная безопасность личности в глобальной информационной среде.

Литература:

1. Мнацаканян А.В. Классификация преступлений против информационной безопасности РФ с точки зрения текущей общественно-политической ситуации // Бизнес в законе. 2014. № 2. С. 270-273.
2. Мнацаканян А.В. Тайна как предмет уголовно-правовой охраны // Социально-политические науки. 2015. № 1. С. 84-87.