

родительского внимания, нехватка общения с членами семьи и т. п.); отсутствие морального и социального воспитания ребенка и др.

Проведенный анализ статистических данных позволяет сделать вывод о том, что тренд снижения преступности несовершеннолетних характерен для обеих стран. Более того, последние годы сильное влияние на несовершеннолетних оказывают социально-экономические, политические, демографические и иные условия. Изложенное обуславливает необходимость проведения всесторонних исследований для выявления реальных причин снижения современной преступности несовершеннолетних, ее латентности и повышения эффективности мер ее предупреждения.

Виноградова Е. С.

ПРОБЛЕМНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ КИБЕРБЕЗОПАСНОСТИ

*Виноградова Екатерина Сергеевна, студентка 4 курса Белорусского
государственного университета, г. Минск, Беларусь,
ekatirina.vinogradova12@gmail.com*

Научный руководитель: канд. юрид. наук, доцент Шидловский А. В.

Национальный сегмент кибербезопасности является составным элементом международной безопасности. Устойчивое функционирование киберпространства является одним из условий обеспечения национальной безопасности, в том числе и Республики Беларусь. Значение развития международного взаимодействия для общего противодействия кибервызовам в последние годы возросло. Однако при построении эффективной системы обеспечения международной кибербезопасности возникает ряд проблем.

Международная кибербезопасность непосредственно связана с киберпространством. Стоит помнить, что если границы территории государства установлены, то границы киберпространства, относящегося к определенному государству, не определены, что существенно влияет на применение норм международного права к отношениям, возникающим в данной области. Осложняется это и тем, что одни государства считают, что каждое государство ответственно за обеспечение безопасности в киберпространстве, которое привязано к территории конкретного государства, а другие – что вопрос обеспечения кибербезопасности нужно решать сообща, посредством закрепления соответствующих положений в международном праве, т. е. в данном случае киберпространство рассматривается как единая среда, не подлежащая делению.

Обеспечение безопасности в киберпространстве осложняется отсутствием механизма понуждения к исполнению норм международного права, регулирующих общественные отношения в киберпространстве, а соответственно, их добровольностью и необязательностью применения.

В вопросах обеспечения международной кибербезопасности важно также обратить внимание на сотрудничество не только между развитыми

странами, но и между развитыми и развивающимися, поскольку, в противном случае, это может привести к появлению «безопасных зон» для киберпреступников. Ведь в большей части для развивающихся стран характерны пробелы в законодательстве и отсутствие надежных мер противодействия киберугрозам, что может повлиять на общую кибербезопасность. Необходимо понимать, что экономическое развитие государства напрямую влияет на его возможности обеспечения сотрудничества такого рода. Неравномерность экономического развития государств и, как следствие, большой разрыв в финансовых и технологических возможностях влияет на эффективность реализации каких-либо действенных мер на практике.

Еще одна проблема заключается в том, что меры, принимаемые на международном уровне, по большей части, носят не профилактический и не предупреждающий характер. Они направлены на уже совершенные преступления и представляют собой определенного рода контрмеры или же действия, которые направлены на пресечение подобного рода преступлений. Одна из первых попыток обеспечить кибербезопасность путем противодействия киберпреступлениям в рамках целой группы государств была сделана в 2001 г. путем подписания Конвенции о преступности в сфере компьютерной информации (Будапештская конвенция). Будапештская конвенция является первым многосторонним юридически обязательным инструментом для регулирования киберпреступности.

Следует понимать, что у каждого государства свой подход к определению того объема общественно опасных действий, которые входят в понятие «киберпреступление». Соответственно, определенные виды деяний могут преследоваться в одном государстве, а в другом – нет, что осложняет процесс взаимного сотрудничества в данном вопросе. Решению данного вопроса способствует принятие региональных нормативных правовых актов, которые и определяют тот объем общественно опасных действий, совершение которых будет уголовно наказуемым. Ярким примером выступает модельный закон «О противодействии киберпреступности» от 14.04.2023 № 55-20, который закрепляет определение киберпреступления и что относится к этим преступлениям. Перечень является открытым, что является положительным в силу динамического развития отношений в киберпространстве и постоянному появлению общественно опасных деяний в данной среде. В целом это определенный толчок к гармонизации законодательства в рамках регионального сотрудничества.

Таким образом, обеспечение кибербезопасности является задачей для каждого государства, которая может быть реализована только с помощью международного партнерства. Устойчивое функционирование и безопасное использование киберпространства возможно лишь на основе международного сотрудничества. Основной площадкой такого сотрудничества должна выступать ООН, объединяющая практически все государства. В этом направлении должны работать также региональные организации, такие как ОДКБ, ШОС, БРИКС и др.