УДК 349

МЕРЫ, ПРИНИМАЕМЫЕ МЕЖДУНАРОДНЫМ СООБЩЕСТВОМ ПО ОХРАНЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Яковенко Екатерина Геннадьевна
Могилевский государственный университет имени А. А. Кулешова
(г. Могилев, Беларусь)

В статье рассматриваются некоторые особенности тех мер, которые принимаются международным сообществом по охране информационной безопасности.

Время стремительного развития компьютерных сетей привело к формированию нового вида преступления – трансграничного компьютерного преступления. Обеспокоенные опасностью того, что компьютерные сети и электронная информация могут также использоваться для совершения преступлений и что доказательства, касающиеся таких преступлений, могут сохраняться и передаваться по этим сетям, представители Совета Европы, а также Соединенных Штатов Америки, Канады и Японии 23 ноября 2001 года подписали Международную Конвенцию по киберпреступности.

Вопрос о борьбе с преступлениями, связанными с использованием компьютеров, был вынесен на повестку дня на XI Конгрессе ООН по

предупреждению преступности и уголовному правосудию в 2005 году. Так, в экспертных рекомендациях был подчеркнут особый характер киберпреступности, необходимость применения комплексных подходов по борьбе с ней и неотложных мер по обновлению уголовного законодательства государств – участников ООН.

Бангкокской декларацией, ставшей результатом деятельности Конгресса, отмечается злоупотребление информационными технологиями и новыми системами телекоммуникаций в преступных целях, целесообразность разработки национальных мер регулирования, что непосредственно отражено в п. 51 Справочного документа семинара-практикума (меры по борьбе против преступлений, связанных с использованием компьютеров). Так, для того, «чтобы эффективно реагировать на запросы о помощи, поступающие от других государств, или получать помощь от других государств, может оказаться необходимым адаптировать национальные законы к задачам борьбы с киберпреступлениями. Совместимость с законами других государств является важной целью при разработке законодательства о борьбе с преступлениями, связанными с использованием компьютеров» [1].

Так, на международном уровне такие организации, как Управление Организации Объединенных Наций по наркотикам и преступности (ЮНОДК или УНП ООН), Международная организация уголовной полиции (Интерпол), Организация международного сотрудничества и развития (ОЭСР) и «группа восьми», а также такие региональные организации, как Европейский союз, Совет Европы, Организация американских государств, Ассоциация государств Юго-Восточной Азии и Азиатско-Тихоокеанская ассоциация экономического сотрудничества (АТЭС), обеспечивают политические и технические знания и опыт, необходимые для развития международного сотрудничества по противодействию киберпреступности.

Очередной организацией, способствующей безопасности в рамках совершения киберпреступлений, является Международная организация уголовной полиции (Интерпол), основной целью которой является объединение всех национальных правоохранительных органов для борьбы с преступностью. Интерпол является так называемым посредником в сотрудничестве правоохранительных органов разных государств в их работе над расследованием и раскрытием преступлений. В этой схеме сотрудничества Интерпол действует как единый центр по разработке совместных полицейских стратегий и тактик борьбы с международной уго-

ловной преступностью. Международная организация уголовной полиции в своей деятельности выделяет сферу киберпреступности, при этом отмечая, что, хотя универсальное определение киберпреступности отсутствует, все преступления данной сферы принято разделять на две группы:

1. *advanced cybercrime* (или высокотехнологичные преступления) – сложные нападения на компьютерные составляющие или программное обеспечение;

2. *cyber-enabled crime* – «традиционные» преступления, которые получили новую форму в связи с развитием Интернета (как, к примеру, преступления, связанные с детьми, экономические преступления, терроризм) [2].

Большинство киберпреступлений носят транснациональный характер, поэтому Интерпол является логичным партнером для любого правоохранительного органа, стремящегося расследовать эти преступления в рамках сотрудничества. Работая с частным сектором, Интерпол способен обеспечить местные правоохранительные органы целенаправленной кибернетической разведкой, полученной путем объединения ресурсов в глобальном масштабе. Основными направлениями деятельности Интерпола в области борьбы с киберпреступностью являются: оперативная и следственная поддержка; киберразведка и анализ; цифровая криминалистика; инновации и исследования; укрепление потенциала и национальные кибер-обзоры.

Одним из составляющих структурных элементов Интерпола являются Национальные центральные бюро, которые находятся и действуют в определенных государствах, наделенные широкими полномочиями по борьбе с преступностью. В соответствии с Постановлением Совета Министров Республики Беларусь № 774 от 10 ноября 1993 года «О совершенствовании мер охраны общественного порядка и борьбы с преступностью» в центральном аппарате Министерства внутренних дел Республики Беларусь создано НЦБ Интерпола в Республике Беларусь.

Необходимо отметить, что деятельность Интерпола по координации международно-правового сотрудничества в борьбе с преступностью в сфере высоких технологий выражается: в правотворческой деятельности Генеральной Ассамблеи Интерпола; в создании специальных подразделений в структуре Интерпола, ответственных за реализацию сотрудничества в борьбе с киберпреступностью в сфере высоких технологий на том или ином участке деятельности; в создании, организации, проведении совместных программ деятельности по пресече-

нию преступности в сфере высоких технологий; в содействии работе правоохранительных органов на национальном уровне путем издания рекомендаций по методикам проведения расследования, проведения совместных конференций для обмена опытом, обучения сотрудников правоохранительных органов.

Таким образом, особенность киберпреступности состоит в том, что одно государство своими силами не может бороться с данным видом преступления, в том числе из-за его транснационального характера. При этом, сотрудничая между собой, международное сообщество в силах противостоять данным преступлениям. Также это обусловлено тем, что в настоящее время информационные ресурсы приравниваются в таким ресурсам, как трудовые, финансовые и иные. Информация стала рассматриваться как нечто материальное, на что преступники могут посягать. Сам транснациональный характер киберпреступности подразумевает под собой разработку общей политики по борьбе с киберпреступлениями. И такая политика должна базироваться на том, что решение данной проблемы состоит в целостном подходе, который подразумевает под собой как развитие национальных мер по борьбе, так и тесное сотрудничество государств на международном уровне.

Список использованных источников

1. Бангкокская декларация [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/documents/decl_conv/declarations/bangkok_declaration.shtml. – Дата доступа: 16.10.2023.
2. The INTERPOL Global Complex for Innovation [Электронный ресурс]. – Режим доступа: https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation. – Дата доступа: 20.10.2023.