

РАЗДЕЛ 2

ГОСУДАРСТВО И ПРАВО. ЮРИСПРУДЕНЦИЯ

Будапештская конвенция о компьютерных преступлениях как инструмент борьбы с киберпреступностью

*Доменикан А. А., студ. III к. БГУ,
науч. рук. Мороз Н. О., канд. юр. наук, доц.*

С развитием информационных технологий и повсеместным распространением доступа к интернету киберпреступность стала одним из самых острых вызовов для мирового сообщества. Всевозрастающая роль компьютерных технологий в сферах обмена информацией и ведения бизнеса в то же время порождает угрозу их злоупотребления в криминальных целях. Для эффективной борьбы с этими угрозами был разработан ряд международных конвенций, одной из которых является Будапештская конвенция о компьютерных преступлениях 2001 г. [1] (далее – Будапештская конвенция).

О необходимости разработки Конвенции по противодействию киберпреступлениям в рамках Совета Европы впервые заговорили в 1997 г., когда стала очевидной их трансграничная направленность и повсеместное распространение [2]. Благодаря конвенции удалось бы достичь не только сближения уголовного законодательства развитых стран в этой сфере, но и стимулирования правотворчества в некоторых развивающихся странах, что в целом привело бы к более эффективному международному сотрудничеству в борьбе с киберпреступлениями [2].

В какой-то степени проблемным вопросом Будапештской конвенции является отсутствие в ней определения понятия «киберпреступление». Вместе с тем конвенция предписывает государствам-участникам принимать в национальном законодательстве специальные меры, направленные против преступных деяний, посягающих на особые выделенные в ней объекты или же совершаемых особыми средствами, то есть, по сути, определение понятия «киберпреступление» дается через его деление.

Так, анализ статей Будапештской конвенции позволяет выделить четыре вида киберпреступлений:

1. *Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.* Среди преступлений, посягающих на данный объект, конвенция называет *противозаконный доступ к компьютерной системе, неправомерный перехват компьютерных данных, неправомерное*

воздействие на данные, неправомерное воздействие на функционирование компьютерной системы и противозаконное использование устройств.

2. *Преступления, связанные с использованием компьютерных средств.* В эту группу включены такие составы, как *подлог с использованием компьютерных технологий и компьютерное мошенничество.*

3. К числу *преступлений относительно содержания данных* Будапештская конвенция относит *различные действия в отношении детской порнографии.* Важной особенностью данного состава в конвенции является криминализация не только действий, носящих коммерческий характер (производство и распространение), но также и самого *владения* детской порнографией, что, к сожалению, не всегда находит отражение в уголовных кодексах некоторых стран.

4. *Преступления, касающиеся нарушения авторского права и смежных прав,* согласно конвенции, имеют место при коммерческом масштабе данных действий с использованием компьютерных систем.

Помимо закрепления отдельных составов киберпреступлений Будапештская конвенция также регулирует следующие вопросы: процессуальные аспекты расследования киберпреступлений, определение юрисдикции по данным преступлениям, а также порядок международного сотрудничества по борьбе с киберпреступностью. Очень важной особенностью Будапештской конвенции является наличие в ст. 24 нормы о выдаче лица, совершившего преступные деяния, установленные конвенцией, при условии, что данное деяние является преступлением по законодательству обеих стран и за него предусмотрено наказание не менее одного года лишения свободы.

Весьма неоднозначное толкование в доктрине получила ст. 32 конвенции, согласно которой сторона конвенции без согласия другой может получить доступ как к общедоступным компьютерным данным вне зависимости от их локализации, так и к данным, хранящимся на территории другой стороны, если есть добровольное согласие лица, способного на законных основаниях раскрывать такие данные. С одной стороны, высказывается мнение, что данная норма «не совсем согласуется с принципом суверенитета и невмешательства во внутренние дела государства, на территории которого находятся интересующие другую сторону электронные данные» [3]. С другой стороны, применение данной нормы возможно обусловить предварительным уведомлением государства о готовящихся или проведенных действиях по сбору данных с территории другого государства [3].

За свою относительно недолгую историю Будапештская конвенция смогла неоднократно продемонстрировать эффективность и получить признание «в качестве наилучшей практики договорно-правового регулирования международного сотрудничества в борьбе с преступностью в сфере высоких технологий» [4]. Благодаря полуоткрытому характеру конвенции ее участниками являются не только члены Совета Европы, но также и Япония, Филиппины,

США, Канада и др. Стоит отметить, что конвенция не учитывала весь возможный масштаб использования компьютерных технологий в преступных целях, что побудило в дальнейшем принятие двух Дополнительных протоколов к Будапештской конвенции, которые, с одной стороны, предусматривали новый состав киберпреступлений – *компьютерные преступления, связанные с актами расизма и ксенофобии*, а с другой стороны, расширяли сотрудничество стран в борьбе с киберпреступностью по различным аспектам.

Таким образом, Будапештская конвенция, несмотря на ее некоторые недостатки, представляет собой важный инструмент в борьбе с киберпреступностью, обеспечивая международное сотрудничество и координацию в области уголовного преследования киберпреступлений. Однако для эффективного противодействия киберугрозам необходимо постоянное развитие и улучшение международных механизмов сотрудничества, а также активное участие государств, международных организаций и частных лиц. Только таким образом можно обеспечить безопасность в киберпространстве и защитить интересы как всего мирового сообщества, так и отдельного индивида.

Литература

1. Конвенция Совета Европы о компьютерных преступлениях [Электронный ресурс] : [заключена в г. Будапеште, 23.11.2001 г.] // Совет Европы : официальный сайт. – Режим доступа: <https://rm.coe.int/1680081580>. – Дата доступа: 27.03.2024.

2. Шестак, В. А. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования [Электронный ресурс] / В. А. Шестак, А. С. Чеботарь // Образование и право. – 2023. – № 8. – Режим доступа: <https://cyberleninka.ru/article/n/budapeshtskaya-konventsia-kak-osnovopolagayuschiy-mehanizm-protivodeystviya-kiberprestupnosti-novatsii-i-perspektivy-mezhdunarodno>. – Дата доступа: 27.03.2024.

3. Клевцов, К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам [Электронный ресурс] / К. К. Клевцов // Вестник СПбГУ. Серия 14. Право. – 2022. – № 3. – Режим доступа: <https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbes-kiberprestupnostyu-v-kontekste-protivodeystviya-novym-vyzovam-i-ugrozam>. – Дата доступа: 29.03.2024.

4. Мороз, Н. О. Особенности участия Республики Беларусь в международном сотрудничестве в сфере обеспечения информационной безопасности [Электронный ресурс] / Н. О. Мороз // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». – 2017. – № 2 (10). – Режим доступа: <https://cyberleninka.ru/article/n/osobennosti-uchastiya-respubliki-belarus-v-mezhdunarodnom-sotrudnichestve-v-sfere-obespecheniya-informatsionnoy-bezopasnosti>. – Дата доступа: 29.03.2024.