Использование компьютерных технологий против личности: подходы к криминализации в странах СНГ

Перина А.С.[1]

Ключевые слова: *уголовная ответственность, модельный закон, преступления против личности, информационно-телекоммуникационные технологии, криминализация, киберпреступность, киберугрозы.*

Аннотация

Цель работы: анализ Модельного Уголовного кодекса (МУК) Содружества Независимых Государств (СНГ), иных международных документов соответствующего регионального международного уровня, а также уголовного законодательства некоторых государств — участников СНГ с точки зрения криминализации преступного использования информационно-телекоммуникационных технологий против личности.

Методы исследования: формально-логический подход к познанию правовых явлений, который позволил установить общие тенденции криминализации, а также методы аналогии, обобщения, дифференциации, сравнительно-правовой и формально-юридический методы.

Результаты исследования: обнаружены различные подходы к установлению уголовной ответственности за преступления против личности, совершенные с использованием компьютерных технологий. Обращено внимание на факт роста пользователей сети Интернет как в мире, так и в России, что обусловливает использование злоумышленниками информационных сетей для совершения преступлений против личности. Приведена краткая сравнительная характеристика использования уголовно-правовых инструментов государствами СНГ для установления ответственности за такие общественно опасные деяния. В результате различного подхода к криминализации возникают значительные недостатки в правовом регулировании киберугроз личности, что указывает на необходимость унификации механизмов реализации уголовно-правовых мер, а также налаживания процесса мониторинга преступлений с использованием компьютерных технологий в целях постоянного получения информации о фактическом состоянии такой преступности как на уровне отдельной страны, так и на международном уровне. Подчеркнуто, что эффективные меры предупреждения должны быть сформулированы на уровне международных нормативных актов СНГ. Отмечается необходимость универсализации и детализации положений о преступном использовании информационно-телекоммуникационных технологий на уровне МУК СНГ, обращения внимания на новые киберугрозы. Предлагается имплементировать подходы некоторых стран к установлению уголовной ответственности за такие преступления в уголовное законодательство других государств СНГ.

Научная новизна: выполнено сравнительное исследование подходов государств СНГ к криминализации общественно опасных деяний против личности, совершаемых с использованием стремительно распространяющихся информационно-телекоммуникационных технологий.

DOI: 10.21681/2226-0692-2023-1-59-68

Введение и постановка задачи

«Мы живем в информационном обществе, в котором широко представлены информационно-телекоммуникационные (компьютерные) технологии»[2].

Использование социальных сетей, возможностей компьютерных технологий, огромный объем информационного пространства в сети Интернет, мессенджеры, электронная почта, мобильные телефоны, покупки онлайн, обмен информацией, поиск единомышленников, виртуальное общение — все это становится неотъемлемой частью жизни общества.

Согласно данным отчета Digital 2022[3], подготовленного организациями We Are Social и Hootsuite, на начало 2022 года 62,5% населения планеты (т. е. 4,95 млрд из 7,91 млрд человек) используют сеть Интернет; указанный показатель по сравнению с предыдущим годом увеличился на 4%. Чуть меньше (4,62 млрд человек) пользуются социальными сетя-

[2] Попов А.Н. Преступления в сфере компьютерной информации : учебное пособие / А. Н. Попов. СПб. : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации. 2018. 68 с.

[3] Simon Kemp. Digital 2022: Local Country Headlines. 26.01.2022. URL: https://datareportal.com/reports/digital-2022-global-overview-report (дата обращения: 05.12.2022).

[1] Перина Анжела Сергеевна, аспирант кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, г. Санкт-Петербург, Российская Федерация. E-mail: anzhela.perina@yandex.ru

ми, в этом случае показатель увеличился на 10% по сравнению с 2021 г.

Согласно указанному отчету, в России эти показатели еще выше. Так, уровень проникновения Интернета в России на начало 2022 г. составил 89% от общей численности населения.

При этом трансграничный характер возможностей в интернет-пространстве, выражающийся в осуществляемом сокрытии географического местоположения собеседника, анонимности доступа к ресурсам, допустимости создания несуществующих личностей, сопряженный с интенсивным развитием навыков пользователей высоких технологий, способствуют уязвимости безопасности личности[4].

Указанные факторы способствуют повышению уровня преступного использования информационно-коммуникационных технологий, что подтверждается статистикой.

В соответствии с отчетом ГИАЦ МВД России[5], содержащим краткую характеристику состояния преступности в Российской Федерации, указано, что за первое полугодие 2022 г. каждое четвертое преступление совершалось с использованием IT-технологий. При анализе группы тяжких и особо тяжких преступлений, совершенных с использованием информационно-телекоммуникационных технологий, наиболее распространенным является использование сети Интернет.

Научное сообщество обеспокоено вопросами распространенности преступлений с использованием компьютерных технологий, в том числе в группе тех, которые направлены против личности. При этом с учетом специфики ее возможностей, выходящих за пределы одного государства, эта проблема приобретает уровень международной.

Стоит также отметить, что использование компьютерных технологий в преступных целях существенно расширилось по сравнению с теми, которые можно было себе представить в начале XXI века. Так, возникает возможность не только хищения персональных данных, кибератак и несанкционированного доступа, но и совершение убийств с помощью современных технологий[6], вербовка жертв через социальные сети для сексуальной эксплуатации, доведение до самоубийства через «группы смерти»[7] и т. д. Иными словами, сегодня объектом посягательства может стать не только компьютер, система и т. п., но и человек как личность, его жизнь и здоровье, половая неприкосновенность, право на неприкосновенность частной жизни и пр.

Необходимость проведения исследования преступного использования высоких технологий против личности подчеркивается и тем, что человек, его права и свободы являются одним из важнейших приоритетов государств, призванного обеспечивать их охрану[8].

Задача настоящего исследования заключается в анализе международных региональных документов на уровне государств — участников Содружества Независимых Государств (далее — СНГ, Содружество), созданного в 1991 году, а также уголовного законодательства государств, входящих в Содружество, на предмет криминализации деяний, направленных против личности, при совершении которых использованы компьютерные технологии.

Результаты исследования

Страны СНГ не находятся в стороне от обозначенной проблемы.

Одним из эффективных методов предупреждения распространения преступного использования компьютерных технологий, повышенная степень общественной опасности которых уже отмечается исследователями[9], является криминализация вновь появляющихся деяний в странах СНГ [1]. Установление уголовной ответственности за совершение преступлений против личности, которые получают все бóльшее распространение ввиду возможностей информационно-коммуникационных технологий, должно отвечать признакам своевременности и отражать реальную ситуацию в обществе. При этом использование компьютерных технологий может быть обозначено в уголовном законодательстве в качестве деяния, отягчающего уголовную ответственность, квалифицирующего признака или как особый способ совершения преступления против личности.

Ученые отмечают, что подходы стран СНГ к криминализации «цифрового» признака в составах тех или иных уголовных правонарушений (проступков и(или) преступлений) являются своего рода способом противодействия «открытым» цифровой трансформацией новым криминальным схемам использования виртуальных технологий [2].

---

[4] Каррыев Б.С., Айдарханов М.Б., Балафанов Е.К. Всемирное Интервидение: Основы информационной культуры : учебно-методическое пособие // Алматы : ИНТ, 2006.

[5] Краткая характеристика состояния преступности в Российской Федерации за январь-июнь 2022 года. URL: https://мвд.рф/reports/item/31209853/ (дата обращения: 05.12.2022).

[6] Кардиостимулятор можно удаленно заставить убить пациента. 17.10.2012. URL: http://hitech.newsru.com/article/17Oct2012/cardio (дата обращения: 22.01.2021).

[7] Зенина М.Г. Лекция на тему «Особенности противодействия преступлениям, связанным с доведением до самоубийства несовершеннолетних с использованием современных информационно-коммуникационных технологий». 2018. URL: https://mvd.ru/upload/site152/folder_page/013/971/704/Lektsiya_p._2.3_Osobennosti_svyazannye_s_dovedeniem_do_samoubiystva.pdf (дата обращения: 01.09.2021).

[8] Всеобщая декларация прав человека, принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 01.08.2021).

[9] Комаров А.А. О критериях общественной опасности, преступлений в сфере высоких технологий / А.А. Комаров // Актуальные вопросы права, экономики и управления : сборник статей IX Международной научно-практической конференции, Пенза, 05 августа 2017 года. Пенза : Наука и просвещение (ИП Гуляев Г.Ю.), 2017. С. 243—245.

DOI: 10.21681/2226-0692-2023-1-59-68

В настоящее время СНГ объединяет: Азербайджанскую Республику, Республику Армения, Республику Беларусь, Республику Казахстан, Кыргызскую Республику, Республику Молдова, Российскую Федерацию, Республику Таджикистан и Республику Узбекистан. С августа 2005 года Туркменистан вышел из действительных членов СНГ и получил статус ассоциированного члена-наблюдателя.

В сфере уголовного права на уровне СНГ одним из существенных документов, подлежащих анализу в рамках исследования, является Модельный Уголовный кодекс, который принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств (постановление № 7-5 от 17 февраля 1996 года) (далее — МУК СНГ).

МУК СНГ к преступлениям против человека относит следующие группы общественно опасных деяний: преступления против жизни и здоровья; преступления против личной свободы, чести и достоинства; преступления против половой неприкосновенности или половой свободы; преступления против конституционных прав и свобод человека и гражданина; преступления против семьи и интересов несовершеннолетних.

Несмотря на то, что указанный документ является рекомендательным актом для стран СНГ, его положения оказали большое влияние на формирование уголовно-правовых норм в соответствующих странах.

Прогрессивным развитием уголовного права в контексте использования компьютерных технологий при совершении преступлений против личности стало Постановление Межпарламентской Ассамблеи СНГ об изменениях в Модельный Уголовный кодекс для государств — участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере № 43-16 от 27 ноября 2015 г.[10], которым внесены некоторые поправки и дополнения.

Так, ст. 151 «Незаконное собирание и распространение информации о частной жизни» дополнена частью второй, в которой указанные действия, если они совершены с использованием компьютерных устройств, системы или их сети, отнесены к преступлениям средней тяжести.

Ст. 153 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» дополнена частью третьей следующего содержания: «(3) Деяния, предусмотренные частью первой или второй настоящей статьи, совершенные с использованием компьютерных устройств, системы или их сети, — преступление средней тяжести.».

Ст. 157 «Фальсификация избирательных документов, документов референдума или неправильный подсчет голосов» дополнена частью второй следующего содержания: «(2) Те же деяния, совершенные с использованием компьютерных устройств, системы или их сети, — преступление средней тяжести.».

Таким образом, на уровне международного документа по указанным составам преступлений против личности подчеркнута повышенная общественная опасность, если они совершены с использованием компьютерных технологий.

Ряд стран имплементировали указанную особенность способа совершения преступлений в свое уголовное законодательство. Например, ч. 2 ст. 178 Уголовного кодекса Республики Молдова (далее — УК Молдовы[11]) закреплено, что за нарушение тайны переписки, телеграмм, посылок и других почтовых отправлений, телефонных переговоров и телеграфных сообщений с нарушением законодательства, совершенное с использованием специальных технических средств, предназначенных для негласного получения информации, предусмотрена повышенная санкция. Уголовный кодекс Республики Казахстан (далее — УК Казахстана) также содержит норму, закрепляющую повышенную ответственность за распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия в средствах массовой информации или с использованием сетей телекоммуникаций, в том числе через Интернет (ч. 5 ст. 147 УК Казахстана).

Составы, касающиеся нарушения неприкосновенности частной жизни, тайны переписки, в Уголовном кодексе Российской Федерации (далее — УК РФ[12]) закреплены в ст. 137—138 и не содержат такого дополнения. Однако ст. 137 УК РФ содержит критерий публичности при совершении незаконного распространения сведений о частной жизни другого лица. При этом ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации, закреплена в отдельной норме (ст. 138.1 УК РФ).

Уголовным кодексом Азербайджанской Республики (далее — УК Азербайджана[13]) при изложении диспозиции ст. 155 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» также не учтен признак использования компьютерных технологий при совершении такого вида преступлений. Однако при формулировании квалифицирующих признаков

[10] Постановление Межпарламентской Ассамблеи СНГ об изменениях в Модельный Уголовный кодекс для государств — участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере № 43-16 от 27.11.2015. URL: https://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=5336 (дата обращения: 01.08.2021).

[11] Уголовный кодекс Республики Молдова от 18.04.2002 № 985-XV. URL: https://online.zakon.kz/Document/?doc_id=30394923 (дата обращения: 01.09.2021).

[12] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.03.2022) (с изм. и доп., вступ. в силу с 23.03.2022) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

13 Уголовный кодекс Азербайджанской Республики (утвержден Законом Азербайджанской Республики от 30.12.1999 № 787-IQ). URL: https://online.zakon.kz/Document/?doc_id=30420353 (дата обращения: 01.09.2021).

состава преступления «Нарушение неприкосновенности частной жизни» законодателем обозначено, что совершение такого общественно опасного деяния «с использованием дистанционно управляемого беспилотного летательного аппарата» влечет повышенную уголовную ответственность (п. 156.2.2 УК Азербайджана). Такой подход представляется прогрессивным, однако является единственным при формулировании диспозиции аналогичного состава преступления в уголовном законодательстве других государств-участников СНГ.

Доведение до самоубийства в рамках МУК СНГ не содержит квалифицирующего признака «с использованием информационно-телекоммуникационных технологий, включая сеть Интернет». Однако такая особенность предусмотрена в УК РФ: п. «д» ч. 2 ст. 110 УК РФ «Доведение до самоубийства»; п. «д» ч. 3 ст. 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства»; ч. 2 ст. 110.2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства». Доведение до самоубийства посредством использования сетей телекоммуникаций, в том числе сети Интернет, криминализировано также в УК Молдовы (ч. 1 ст. 150[14]), УК Казахстана (п. 4 ч. 2 ст. 105[15]). При этом, например, Уголовный кодекс Армении (ст. 110[16]) и Уголовный кодекс Республики Таджикистан (ст. 109[17]) при установлении уголовной ответственности за аналогичные деяния не содержит выделения квалифицированного состава с признаком «совершенное с использованием информационно-телекоммуникационных сетей».

Таким образом, ряд стран в рамках внутригосударственной уголовной политики, независимо от отсутствия в МУК СНГ рекомендательных норм об ответственности за преступления, совершенных с использованием компьютерных технологий, придерживаются позиции необходимости усиления уголовной ответственности за такие преступления, направленные против личности, поскольку деструктивное воздействие интернет-пространства и информационно-коммуникационных технологий ставит под угрозу безопасность граждан.

Такой подход применим в ряде стран СНГ и для преступлений против несовершеннолетних, при совершении которых используется информационно-телекоммуникационная сеть, ввиду того что несовершеннолетние являются категорией населения, нуждающейся в особой уголовно-правовой защите. На международном региональном уровне рекомендовано установление повышенных мер уголовной ответственности за любые формы нравственного растления, сексуального совращения и эксплуатации детей, злоупотребление их беспомощным или зависимым состоянием, если это совершено с использованием средств массовой информации и информационно-телекоммуникационных сетей[18].

Так, положениями ст. 175-1 УК Молдовы[19] криминализировано следующее деяние: «Обольщение несовершеннолетнего в сексуальных целях», а именно: предложение, убеждение, манипулирование, угроза, обещание выгод в любой форме, осуществляемые в том числе посредством информационных технологий или средств электронных коммуникаций, с целью назначения встречи с несовершеннолетним для совершения в отношении него любого рода преступления, относящегося к половой сфере, если за такими действиями последовали конкретные деяния, ведущие к такой встрече, наказываются лишением свободы на срок от 2 до 6 лет.

В УК Казахстана в раздел преступлений против личности включена ст. 134 «Вовлечение несовершеннолетнего в занятие проституцией». Так, ч. 3 указанной статьи криминализировано указанное деяние посредством использования сетей телекоммуникаций, в том числе сети Интернет[20].

УК РФ в связи с недавними изменениями закреплена повышенная ответственность за понуждение к действиям сексуального характера с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «б» ч. 3 ст. 133 УК РФ[21]), что отражает попытку государства обеспечить охрану половой неприкосновенности несовершеннолетних уголовно-правовыми средствами.

В России криминализировано также склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, совершенное в публичном

[14] Уголовный кодекс Республики Молдова от 18.04.2002 № 985-XV. URL: https://online.zakon.kz/Document/?doc_id=30394923 (дата обращения: 01.09.2021).

[15] Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V. URL: https://online.zakon.kz/Document/?doc_id=31575252#pos=1675;-26 (дата обращения: 01.09.2021).

[16] Уголовный кодекс Республики Армения от 29 апреля 2003 года № ЗР-528. URL: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus (дата обращения: 01.09.2021).

[17] Уголовный кодекс Республики Таджикистан от 21.05.1998 № 574. URL: https://online.zakon.kz/Document/?doc_id=30397325 (дата обращения: 01.09.2021).

[18] Пункт 6.2.3 Рекомендаций по гармонизации и унификации законодательства государств — участников СНГ в сфере защиты детей от информации, причиняющей вред их здоровью и развитию, принятых на тридцать пятом пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление № 35-8 от 28 октября 2010 года). URL: https://iacis.ru/public/upload/files/1/333.pdf (дата обращения: 05.09.2021).

[19] Уголовный кодекс Республики Молдова от 18.04.2002 № 985-XV. URL: https://online.zakon.kz/Document/?doc_id=30394923 (дата обращения: 01.09.2021).

[20] Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V. URL: https://online.zakon.kz/Document/?doc_id=31575252#pos=1675;-26 (дата обращения: 01.09.2021).

[21] Федеральный закон от 06.03.2022 № 38-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 280 Уголовно-процессуального кодекса Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru. 6 марта 2022 г. № 0001202203060004.

DOI: 10.21681/2226-0692-2023-1-59-68

выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет) в соответствии с п. «в» ч. 2 ст. 151.2 УК РФ. Такого состава нет ни в одном из уголовных законов других стран СНГ.

В ряде стран криминализировано преступное использование сети Интернет в целях оскорбить человека или опорочить честь и достоинство личности.

Например, ст. 147.1 УК Азербайджана предусмотрена ответственность за распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или, при массовом распространении, в информационном ресурсе Интернета. При этом ст. 148-1 УК Азербайджана закреплен следующий состав преступления: клевета или оскорбление в информационном интернет-ресурсе с использованием поддельных имен пользователя, профилей или учетных записей (таких, которые не позволяют идентифицировать личность пользователя, т. е. созданы с размещением ложных данных об имени, фамилии или отчестве либо путем сокрытия этой информации, а также с использованием сведений, относящихся к другому лицу, без согласия последнего[22]). Соответствующий опыт может быть распространен и в уголовное законодательство других государств СНГ, в том числе России.

В соответствии с УК РФ такое деяние не криминализировано. Более того, в 2011 году состав «Оскорбление» был декриминализирован и перенесен в разряд административных правонарушений. Однако имеющаяся тенденция оскорбления в сети Интернет, возможность распространения оскорбительных видео- или фотоматериалов о человеке могут нанести ущерб не только его репутации, но и его психическому здоровью. Можно отметить кибербуллинг, имеющийся в подростковой среде, который может повлиять на жизнь и здоровье ребенка, при этом уголовная ответственность за унижение чести и достоинства личности может не наступить при отсутствии признака состава доведения до самоубийства, например, или клеветы.

Ст. 188 Уголовного кодекса Республики Беларусь[23] в рамках криминализации преступлений против личности установлена уголовная ответственность за клевету, содержащуюся в информации, размещенной в глобальной компьютерной сети Интернет[24].

Еще один документ, принятый на международном уровне, который закрепляет положения о киберпреступности — это Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[25], подписанное 28 сентября 2018 г. на заседании Совета глав государств СНГ и заменившее существовавшее ранее Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г. Вновь принятое соглашение актуализировано в контексте появления новых видов преступлений, связанных с развитием информационно-телекоммуникационных технологий.

Целесообразность ратификации указанного документа международного характера Россией, обусловленная потребностью в расширении правовых основ сотрудничества правоохранительных и судебных органов государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации, отмечалась некоторыми учеными[26].

Относительно недавно, 1 июля 2021 г., Россия ратифицировала (с оговоркой[27]) указанный международный документ, созданный в целях борьбы с преступлениями, совершенными с использованием компьютерных технологий. Однако указанный документ тоже подробно не раскрывает преступное использование компьютерных технологий против личности.

Существуют составы преступлений против личности, которые могут быть приняты во внимание в контексте все более активного использования при их совершении компьютерных технологий и социальных сетей, что способствует повышению их общественной опасности.

Так, несмотря на то, что на международном уровне отмечалась проблема торговли людьми, в настоящее время аспект использования компьютерных технологий и социальных сетей при совершении указанного преступления не рассмотрен основательно с точки зрения установления уголовной ответственности.

В ходе анализа фабулы судебных дел, которые отражены в Глобальным докладе Управления ООН по наркотикам и преступности (UNODC) о торговле

---

[22] Уголовный кодекс Азербайджанской Республики (утвержден Законом Азербайджанской Республики от 30.12.1999 № 787-IQ). URL: https://online.zakon.kz/Document/?doc_id=30420353 (дата обращения: 01.09.2021).

[23] Уголовный кодекс Республики Беларусь от 09.07.1999 № 275-З. URL: https://online.zakon.kz/Document/?doc_id=30414984 (дата обращения: 01.09.2021).

[24] Семыкина О. И. Противодействие киберпреступности за рубежом / О. И. Семыкина // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6(61). С. 104—113. DOI: 10.12737/23525 .

[25] Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий. 28.09.2018. URL: https://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=5864 (дата обращения: 15.08.2021).

[26] Ястребов Д.А. Международно-правовое сотрудничество государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Юридический мир. 2008. № 12. С. 73—77.

[27] Федеральный закон от 01.07.2021 № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru. 01.07.2021. № 0001202107010016.

людьми за 2020 год[28], установлено, что социальные сети, компьютерные технологии зачастую используются при обозначенном составе преступления для вербовки жертв, рекламирования услуг людей, находящихся в результате таких сделок в сексуальном рабстве, бесконтактному общению между продавцами, жертвами, покупателями и пр.

Так, в Беларуси осужден злоумышленник, который организовал каналы торговли девушек модельной внешности из Беларуси, Украины, Российской Федерации и Казахстана в Турцию для занятия проституцией. Все контакты между членами преступной группы и торговцами людьми, а также вербовка девушек проводилась через Интернет, без личных встреч или передачи наличных денег. Социальная сеть «ВКонтакте» была использована для вербовки путем создания вымышленных личностей, различных групп, рекламирующих работу в Турции с высоким заработком в модельном бизнесе без проституции. Девушки, которых привлекли эти предложения, представили свои фотографии в бикини, а также обнаженными и частично обнаженными одному из вербовщиков. Злоумышленники, используя сервис обмена сообщениями Viber, отправляли фотографии минским торговцам людьми на утверждение. После одобрения девушкам сообщалась правда о необходимости оказания сексуальных услуг за деньги. В случае отказа фотографии обнаженных девушек использовались для их шантажа. За девушек, которые соглашались, денежные средства переводились также без личных встреч посредством сервиса Western Union и MoneyGram. Таким образом, продажа более 100 девушек осуществлялась посредством социальных сетей и мессенджеров полностью бесконтактно, без каких-либо личных встреч был организован их перелет, контроль, проживание и пр.[29] Такие дела демонстрируют отсутствие необходимости физических контактов для взаимодействия при совершении преступлений против личности при наличии социальных сетей и мессенджеров. Аналогичные случаи наблюдались и в России.

Зачастую торговля людьми носит трансграничный характер и приобретает новые формы. Сексуальное совращение и эксплуатация потенциальных жертв торговли людьми с использованием СМИ, информационно-телекоммуникационных сетей (Интернета, мобильной связи) может происходить и без пересечения границ государств, путем принудительного выполнения указанных действий в рамках онлайн-трансляций; участились случаи обмена собственными изображениями сексуального характера [3] и пр. Такой аспект повышает общественную опасность указанных видов преступлений и нуждается в особом внимании с точки зрения закрепления соответствующей ответственности.

Постановлением Межпарламентской Ассамблеи СНГ об изменениях и дополнениях в модельные Уголовный и Уголовно-процессуальный кодексы для государств — участников СНГ по вопросам борьбы с торговлей людьми № 39-24 от 29.11.2013 в Модельный Уголовный кодекс введена статья 140.1, которая содержит положения о тяжести преступления, выражающегося в торговле людьми. При этом ни часть 2, ни часть 3 указанной статьи, отражающие квалифицирующие признаки, не содержат норму о совершении такого деяния с использованием компьютерных технологий.

Вместе с тем ввиду указанной международной практики возникает целесообразность включения в часть 2 статьи 140.1 Модельного Уголовного кодекса под пунктом «с» дополнительного квалифицированного состава соответствующего преступления: «с использованием информационно-телекоммуникационных технологий, социальных сетей или иным аналогичным способом».

Ряд ученых отмечают, что «распространение в последнее десятилетие новых, нетрадиционных форм и способов торговли людьми, в том числе с использованием информационных технологий, обусловливает потребность в унификации подходов государств — участников СНГ к криминализации и пенализации общественно опасных деяний в указанной сфере за счет введения в уголовные кодексы государств норм об ответственности за соответствующие виды преступлений в сфере электронной информации»[30].

Пропаганда преступлений, связанных с торговлей людьми, включая пропаганду порнографии, проституции, иных коммерческих сексуальных услуг и распространение в средствах массовой информации, телекоммуникационных сетях рекламной продукции и иной информации, способствующей виктимизации потенциальных жертв торговли людьми, также рекомендована к закреплению в национальном уголовном законодательстве положениями международного характера[31].

При этом в документах международного характера регионального уровня уже подчеркнуто, что в сфере борьбы с торговлей людьми уголовные

---

[28] Global Report on Trafficking in Persons. 2020. URL: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf (дата обращения: 15.08.2021).

[29] Collection of Court Case Summaries // Global Report on Trafficking in Persons. 2020. URL: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTIP_2020_Court_Cases_Summaries.pdf (дата обращения: 01.07.2022).

[30] Винокуров С.И., Пристанская О.В. Научный комментарий к Модельному закону «О противодействии торговле людьми». Приложение к постановлению МПА СНГ от 23 ноября 2012 г. № 38-19. С. 107. URL: https://iacis.ru/public/upload/files/1/375.pdf (дата обращения 15.03.2022).

[31] Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющий Конвенцию ООН против транснациональной организованной преступности, принят резолюцией 55/25 Генеральной Ассамблеи ООН от 15 ноября 2000 г., ратифицирован Российской Федерацией (Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» от 26 апреля 2004 г. № 26-ФЗ). URL: https://www.un.org/ru/documents/decl_conv/conventions/protocol1.shtml (дата обращения: 01.12.2022).

DOI: 10.21681/2226-0692-2023-1-59-68

санкции могут быть ужесточены за любые формы совращения, злоупотреблений и эксплуатации детей, в том числе с использованием средств массовой информации, информационно-телекоммуникационных сетей открытого доступа и в иных публичных формах[32].

На уровне СНГ также принят Модельный закон «О противодействии торговле людьми», в котором подчеркнута важность мониторинга в сфере торговли людьми путем мониторинга сети Интернет и мобильной связи, а также описаны меры по предупреждению и противодействию осуществления торговли людьми, в том числе посредством информационно-телекоммуникационных технологий[33].

Установление ответственности за такое деяние, совершенное с использованием информационно-телекоммуникационных средств, даже на уровне рекомендованного для нескольких стран состава преступления станет шагом вперед на пути к признанию повышенной общественной опасности преступления и отвечает международно-правовым принципам, ориентирующим государства на существенное ужесточение ответственности за любые формы сексуальной эксплуатации детей в информационно-телекоммуникационных сетях, включая соблазнение ребенка в режиме онлайн с целью организации свидания и совершения сексуального преступления, в том числе в различных странах, а также детскую проституцию, организуемую через Интернет.

Выводы

Таким образом, анализ вышеупомянутых международных документов, направленных на борьбу с киберпреступностью, показал, что, несмотря на принятие указанных документов международного характера, уголовное законодательство стран СНГ, как и практика по борьбе с таким видом преступлений пока не получили достаточно глубокой разработки и отражают лишь отдельные аспекты проблемы, носят фрагментарный характер. Это выражается в региональном характере регулирования вопросов криминализации цифровой преступности, индивидуальном отношении каждой страны к проблеме, а также в отсутствии полноценного отражения основных способов криминального использования компьютерных технологий, которые сегодня стремительно развиваются. Такой подход приводит к отличию в уголовной политике отдельных стран СНГ по установлению ответственности за совершение преступлений против личности, объективная сторона которых включает использование информационно-телекоммуникационных технологий.

В понимании границ информационного преступления, включает ли оно понятие преступлений с использованием компьютерных технологий, также нет единого подхода ни среди исследователей [4], ни на уровне международных документов. Отсутствует и единое понимание перечня составов преступлений, которые совершаются с использованием компьютерных технологий. Вопросы необходимости криминализации соответствующих деяний, выделения общих квалифицирующих признаков, обозначения единых признаков составов преступлений, совершенных с использованием информационно-коммуникационных технологий, для всех стран — участниц СНГ остаются нерешенными. Это применимо и к преступлениям против личности. Такая разрозненность в уголовно-правовой сфере на международном региональном уровне способствует отсутствию единообразного понятийного аппарата, усложняющего сотрудничество государств по различным вопросам противодействия преступлениям в сфере цифровой преступности, установления ответственности за общий перечень аналогичных преступных деяний. Так, преступления могут быть совершены с помощью компьютерных технологий в стране, которая не предусматривает в качестве преступного такое деяние, что может привести к безнаказанности или возможным правовым конфликтам между странами, а также к неоднозначному подходу к вопросам выдачи преступников и пр.

Обозначенные вопросы, касающиеся преступлений против личности, не решены и на уровне МУК СНГ, хотя заслуживают внимания ввиду возрастающей возможности их совершения с использованием достижений научно-технического прогресса.

Исследователи Р. Вудхед, П. Стивенсон и Д. Морри отмечают, что развитие цифровых технологий сильно влияет на Стратегию цифровой экономики в целом [5], которая имеет немаловажное значение на территории стран СНГ. Такой подход является еще одним аргументом активизации детальной проработки проблемы криминализации преступного использования компьютерных технологий, в том числе направленных против личности.

В качестве одной из задач решения проблемы некоторые ученые отмечают важность создания универсального международно-правового механизма противодействия преступному использованию компьютерных технологий [6] и разработки универсальных норм в российском законодательстве, адаптированных к новым видам цифровых угроз [7]. Представляется верным, что создание универсальных норм на уровне международного регионального права является очевидным и немаловажным процессом [8], поскольку единообразие уголовно-

---

[32] Рекомендации по унификации и гармонизации законодательства государств — участников СНГ в сфере борьбы с торговлей людьми. Приняты на тридцатом пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление № 30-13 от 03.04.2008).

[33] Модельный закон государств — участников СНГ «О противодействии торговле людьми». Принят на 30 пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление от 03.04.2008 № 30-11). URL: https://iacis.ru/public/upload/files/1/232.pdf (дата обращения: 01.12.2022).

правовых норм имеет положительный правовой эффект. Одним из вариантов решения такой задачи может стать разработка и создание универсальной международной конвенции, учитывая трансграничный характер такого рода преступности, что станет серьезным подспорьем для национального законодательства. Некоторыми исследователями [9] предлагается создание универсального международного договора, который смог бы объединить положения о единообразном подходе к криминализации деяний на территории стран СНГ, взаимодействие государств на уровне решения вопросов предупреждения преступного использования компьютерных технологий, которое выходит за пределы одного государства, и т. д., что будет иметь явный положительный правовой эффект. Такой универсальный международно-правовой документ, отражающий существующее реальные угрозы, должен носить не только характер констатирующего уже вошедшую в повседневную жизнь киберпреступность, но и предупреждающий характер.

Справедливо подчеркивается важность обмена статистической информацией о состоянии преступности[34], что возможно при внедрении процесса мониторинга преступлений с использованием компьютерных технологий, позволяющего получать информацию о фактическом состоянии такой преступности как на уровне отдельной страны, так и на международном уровне.

Кроме того, положения, отражающие перечень случаев преступного использования компьютерных технологий, созданные на уровне международного документа, позволят государствам имплементировать в национальное законодательство более конкретные формулировки таких преступлений, исключив различный подход со стороны разных стран СНГ.

Меры по предупреждению распространения обозначенного в исследовании вида преступлений не могут проходить и без взаимодействия государств с институтами гражданского общества, включая общественные объединения, средства массовой коммуникации [10] и т. д.

Представляется аргументированным подход ученых, заключающийся в необходимости дальнейшего развития и совершенствования организационных и правовых механизмов, законодательных конструкций в рассматриваемой сфере в странах СНГ, что позволит повысить уровень и эффективность межгосударственного сотрудничества в борьбе с киберпреступностью на обозначенном уровне[35]. Кроме того, выделение в статистических данных количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, целесообразно с точки зрения важности организации более качественного и детального исследования такого вида преступлений. Такой подход позволит также анализировать их более комплексно, демонстрировать динамику совершенных преступлений в сфере телекоммуникаций и проследить тенденции применения в преступных целях к разным категориям общественных отношений, в том числе против личности.

Результаты исследования уголовного законодательства указанных стран СНГ свидетельствуют о том, что необходимо постоянно совершенствовать правовые конструкции МУК СНГ, использовать опыт стран, криминализировавших те или иные деяния, направленные против личности и при совершении которых использованы компьютерные технологии, как для отечественного уголовного законодательства, так и для иных государств СНГ. Например, в рамках совершенствования МУК СНГ, а также национального уголовного законодательства стран — участниц Содружества может быть принято во внимание установление уголовной ответственности за преступления, касающиеся обольщения несовершеннолетнего в сексуальных целях с использованием информационно-коммуникационных технологий. Кроме того, имплементация норм об оскорблении в сети Интернет, причиняющем вред здоровью личности, а также использование при совершении тех или иных «традиционных» преступлений компьютерных технологий может быть использована в рамках Общей части уголовного закона в качестве признака, отягчающего наказание, поскольку перечень составов преступлений против личности с использованием информационно-телекоммуникационных средств стремительно расширяется.

---

[34] Ревин В.П. Актуальные проблемы сотрудничества государств — участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий / В.П. Ревин // Международное сотрудничество евразийских государств: политика, экономика, право. 2017. № 1 (10). С. 83—91.

[35] Мукашев С.И. Международно-правовое сотрудничество государств — участников СНГ в борьбе с преступностью в сфере компьютерной информации / С. И. Мукашев // Право.by. 2014. № 5 (31). С. 81—86.

DOI: 10.21681/2226-0692-2023-1-59-68

Литература

1. Голованова Н.А. Новые формы онлайн-преступности за рубежом / Н.А. Голованова // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3 (76). С. 42—57. DOI: 10.12737/jflcl.2019.3.4 .
2. Семыкина О.И. «Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств — участников СНГ) / О.И. Семыкина, Р.Н. Ключко // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 6 (85). С. 34—52. DOI: 10.12737/jflcl.2020.051 .
3. Коваленко В.И. Межгосударственное сотрудничество государств — участников Содружества Независимых Государств по противодействию торговле людьми и криминальной эксплуатации человека / В.И. Коваленко // Военное право. 2021. № 2 (66). С. 295—301.
4. Лукьянов Н.Е. Законодательное регулирование ответственности за информационные преступления. Зарубежный опыт / Н.Е. Лукьянов // Устойчивое развитие науки и образования. 2019. № 2. С. 134—139. EDN: YZCUWD.
5. Woodhead R. Digital construction: From point solutions to IoT ecosystem / R. Woodhead, P. Stephenson, D. Morrey. DOI: 10.1016/j.autcon.2018.05.004 // Automation in Construction. 2018. № 93. С. 35—46.
6. Мороз Н.О. Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС / Н.О. Мороз // Вестник Марийского государственного университета. Серия: Исторические науки. Юридические науки. 2018. Т. 4. № 4 (16). С. 87—95. DOI: 10.30914/2411-3522-2018-4-4-87-94 .
7. Бегишев И.Р. Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере / И.Р. Бегишев, З.И. Хисамова // Baikal Research Journal. 2019. Т. 10. № 3. С. 15. DOI: 10.17150/2411-6262.2019.10(3).15 .
8. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е.А. Русскевич // Международное уголовное право и международная юстиция. 2018. № 3. С. 10—13.
9. Мысина А.И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий / А.И. Мысина // Международное право. 2019. № 1. С. 18—27. DOI: 10.25136/2306-9899.2019.1.29027 .
10. Никеров Д.М. Преступления в сфере высоких технологий в современной России / Д.М. Никеров, О.М. Хохлова // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2019. № 2 (89). С. 82—93. DOI: 10.24411/2312-3184-2019-00008 .

Using computer technologies against persons: approaches to criminalisation in the countries of the Commonwealth of Independent States

Anzhela Perina[36]

Keywords: *criminal responsibility, model law, offences against persons, information and telecommunication technologies, criminalisation, cybercrime, cyber threats.*

Abstract

Purpose of the paper: analysing the Model Criminal Code (MCC) of the Commonwealth of Independent States (CIS) and other international documents of an appropriate regional international level as well as the criminal laws of some member countries of the CIS from the viewpoint of criminalisation of misuse of information and telecommunication technologies against persons.

Methods of study: the formal logical approach to the cognition of legal phenomena which allowed to find out the general tendencies in criminalisation as well as methods of analogy, generalisation, differentiation, and the comparative legal and formal legal methods.

Study findings: different approaches to establishing criminal responsibility for offences against persons involving the use of computer technologies were identified. Attention is drawn to the growth of the number of Internet users both in the world at large and in Russia which brings about using information networks by wrongdoers for committing offences against persons. A brief comparative description of using criminal law tools by CIS countries to establish responsibility for such socially dangerous acts is given. As a result of different approaches to criminalisation, considerable drawbacks

[36] Anzhela Perina, Ph.D. student at the Department of Criminal Law, Criminology and Penitentiary Law of the Saint Petersburg Law Institute (branch) of the University of the Prosecution Service of the Russian Federation, Saint Petersburg, Russian Federation. E-mail: anzhela.perina@yandex.ru

in the legal regulation of cyber threats against persons emerge which points to a need to unify the mechanisms for implementing criminal law measures as well as to set up monitoring of crimes using computer technologies with a view to continuously getting information on the actual situation with these crimes on the level of individual countries as well as on the international level on the whole. It is emphasised that efficient prevention measures must be worded on the level of international legal regulations of the CIS. A need for the universalisation and detalisation of provisions on the criminal use of information and telecommunication technologies at the level of the MCC of the CIS as well as placing attention on new cyber threats are noted. It is proposed to implement the approaches to establishing criminal responsibility for such offences adopted by some countries in the criminal law of other CIS countries.

Research novelty: a comparative study of approaches of CIS countries to the criminalisation of socially dangerous acts against persons committed with the use of fast-spreading information and telecommunication technologies was carried out.

References

1. Golovanova N.A. Novye formy onlain-prestupnosti za rubezhom. N.A. Golovanova. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia, 2019, No. 3 (76), pp. 42–57. DOI: 10.12737/jflcl.2019.3.4 .
2. Semykina O.I. "Tsifrovoi" priznak sovershenіia prestuplenii kak vektor kriminalizatsii (komparativnyi obzor podkhodov gosudarstv – uchastnikov SNG). O.I. Semykina, R.N. Kliuchko. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia, 2020, No. 6 (85), pp. 34–52. DOI: 10.12737/jflcl.2020.051 .
3. Kovalenko V.I. Mezhgosudarstvennoe sotrudnichestvo gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv po protivodeistviiu torgovle liud'mi i kriminal'noi ekspluatatsii cheloveka. V.I. Kovalenko. Voennoe pravo, 2021, No. 2 (66), pp. 295–301.
4. Luk'ianov N.E. Zakonodatel'noe regulirovanie otvetstvennosti za informatsionnye prestupleniia. Zarubezhnyi opyt. N.E. Luk'ianov. Ustoichivoe razvitie nauki i obrazovaniia, 2019, No. 2, pp. 134–139. EDN: YZCUWD.
5. Woodhead R. Digital construction: From point solutions to IoT ecosystem. R. Woodhead, P. Stephenson, D. Morrey. DOI: 10.1016/j.autcon.2018.05.004. Automation in Construction, 2018, No. 93, pp. 35–46.
6. Moroz N.O. Osobennosti mezhdunarodno-pravovogo sotrudnichestva v bor'be s kiberprestupnost'iu v ramkakh ES. N.O. Moroz. Vestnik Mariiskogo gosudarstvennogo universiteta, seriia: Istoricheskie nauki. Iuridicheskie nauki, 2018, t. 4, No. 4 (16), pp. 87–95. DOI: 10.30914/2411-3522-2018-4-4-87-94 .
7. Begishev I.R. Sravnitel'no-pravovoi analiz zakonodatel'stva Velikobritanii i Rossii v oblasti protivodeistviia prestupleniiam v tsifrovoi sfere. I.R. Begishev, Z.I. Khisamova. Baikal Research Journal, 2019, t. 10, No. 3, pp. 15. DOI: 10.17150/2411-6262.2019.10(3).15 .
8. Russkevich E.A. Mezhdunarodno-pravovye podkhody protivodeistviia prestupleniiam, sovershaemym s ispol'zovaniem informatsionno-kommunikatsionnykh tekhnologii. E.A. Russkevich. Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaia iustitsiia, 2018, No. 3, pp. 10–13.
9. Mysina A.I. Mezhdunarodno-pravovye osnovy sotrudnichestva gosudarstv po protivodeistviiu prestupleniiam v sfere informatsionnykh tekhnologii. A.I. Mysina. Mezhdunarodnoe pravo, 2019, No. 1, pp. 18–27. DOI: 10.25136/2306-9899.2019.1.29027 .
10. Nikerov D.M. Prestupleniia v sfere vysokikh tekhnologii v sovremennoi Rossii. D.M. Nikerov, O.M. Khokhlova. Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennikh del Rossii, 2019, No. 2 (89), pp. 82–93. DOI: 10.24411/2312-3184-2019-00008 .

DOI: 10.21681/2226-0692-2023-1-59-68