«Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств — участников СНГ)

СЕМЫКИНА Ольга Ивановна, старший научный сотрудник отдела зарубежного конституционного, административного, уголовного законодательства и международного права Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, кандидат юридических наук

Россия, 117218, г. Москва, ул. Большая Черемушнская, 34

E-mail: semykola@yandex.ru

КЛЮЧКО Римма Николаевна, заведующая кафедрой уголовного права, уголовного процесса и криминалистики Гродненского государственного университета им. Янки Купалы, кандидат юридических наук, доцент

Республика Беларусь, 230023, г. Гродно, ул. Ожешко, 22

E-mail: klrn.grodno@tut.by

Цифровые технологии, создающие огромные возможности для повышения скорости и изменения форм информационного взаимодействия между различными субъектами общественных отношений (информатизации), порождают изменение их содержания. Поиск, получение, передача, сбор, обработка, накопление, хранение, распространение, предоставление, использование и защита информации, применение цифровых и иных информационно-телекоммуникационных технологий для этих же действий сформировали «суперинститут» информационных отношений, который требует адекватных мер защиты от неправомерного воздействия и нарушения конфиденциальности. Правовое регулирование информационных отношений должно обеспечивать их развитие с учетом потребностей различных субъектов, а уголовно-правовая охрана — состояние защищенности информационной безопасности и информационного суверенитета соответствующих субъектов, предупреждение нарушений правового статуса соответствующих субъектов и противодействие использованию «цифровых» объектов в криминальных целях.

Интенсивная цифровая трансформация меняет подход к пониманию прежде всего информационной безопасности. Сегодня информационная безопасность, во-первых, является неотъемлемым элементом информационных отношений, во-вторых, сопряжена с обеспечением информационного суверенитета и, в-третьих, выступает дополнительным объектом всех преступлений против прав, свобод и законных интересов личности, общества и государства, совершаемых посредством цифрового воздействия. Такое понимание информационной безопасности позволило авторам предложить корректировки модельного уголовного законодательства для государств — участников СНГ и уголовных законов некоторых членов этого интеграционного объединения (на примере Российской Федерации и Республики Беларусь) в части пересмотра подходов к определению объекта уголовно-правовой охраны от собственно киберправонарушений.

С использованием компаративного, аналитического и экстраполяционного методов освещаются особенности криминализации в Модельном уголовном кодексе для государств — участников СНГ и в национальных уголовных кодексах соответствующих стран двух групп уголовных правонарушений — собственно киберправонарушений и правонарушений информационного характера. Особое внимание уделено установлению ответственности за те деяния, входящие в обозначенные группы уголовных правонарушений, которые обладают необходимым уровнем новации и отвечают глобальным вызовам и угрозам со стороны оправдания деструктивной идеологии и нарушения общественного порядка.

Ключевые слова: уголовный кодекс, модельный закон, киберправонарушение, правонарушение информационного характера, информационные отношения, информационная безопасность, информационный суверенитет, деструктивное информационно-телекоммуникационное воздействие, «цифровой» признак преступления.

Для цитирования: Семькина О. И., Ключко Р. Н. «Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств — участников СНГ) // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 6. С. 34—52. DOI: 10.12737/jflcl.2020.051

Интенсивное расширение сферы адаптации криминообразующего «цифрового» признака в уголовных кодексах государств — участников СНГ можно признать мегатрендом трансформации современной уголовной политики этих стран. Актуальность компаративного обзора подходов к реальному воплощению этого мегатренда обусловлена глобализацией рисков и угроз от бесконтрольного использования виртуальных возможностей для информационной безопасности и информационного суверенитета субъектов информационных отношений. И если основы предупреждения рисков закладываются в меж-

отраслевых регулятивных механизмах, то борьба с существующими вредоносными угрозами — в репрессивных средствах «жесткого права», формулирующих уголовно-правовые запреты на неправомерные изменения содержания и формы цифровой информации, применение информационно-телекоммуникационных технологий и сетевых ресурсов, технических средств и оборудования в качестве «цифрового оружия». Такие запреты должны блокировать любую — как формальную, так и материальную — возможность причинения ущерба «классической триаде» субъектов общественных отношений (личности, обществу

и государству) и деструктивного информационного воздействия на них¹. С этих позиций несомненный интерес для законодателя, ученого и практика представляет освещение подходов государств — участников СНГ к криминализации «цифрового» признака в составах тех или иных уголовных правонарушений (проступков и(или) преступлений) как способу противодействия «открытым» цифровой трансформацией новым криминальным схемам использования виртуальных технологий.

В уголовных кодексах государств — участников СНГ выделяются две крупные группы уголовных правонарушений, при совершении которых для воздействия на охраняемый объект используются цифровые и иные информационно-телекоммуникационные технологии: 1) собственно киберправонарушения (проступки и(или) преступления в сфере информатизации и связи); 2) правонарушения информационного характера, где «цифровой» признак (сопряженность с информатизацией) встроен в оболочку так называемых традиционных (общеуголовных) преступлений и отражает их информационную направленность (обусловленность).

Конечно, как и любая научная классификация, предлагаемое двучленное деление деяний², в составе которых так или иначе присутствует «цифровой» признак, является условным и экстраполируется на законодательство не всех государств. Например, исследователь уголовного права Великобритании Н. А. Голованова выделяет сходную модель разделения уголовных правонарушений такого рода, дифференцируя: 1) компьютерные преступления в «чистом

виде», связанные с использованием компьютерных технологий, когда компьютер выступает как цель или инструмент посягательства³; 2) «традиционные» деяния, в которых для достижения преступных намерений используются компьютеры, компьютерные сети или иные формы информационно-телекоммуникационных технологий (где особо актуальны посягательства на личность, мораль, имущественные преступления и др.⁴). Вместе с тем встречаются и более широкие классификации. Так, рассматривая правовую систему США, С. П. Кубанцев разграничивает три направления преступной деятельности: 1) преступления, сопряженные с использованием киберпространства как вспомогательного фактора, например для поиска и привлечения сообщников и координации преступных действий; 2) деяния, совершаемые непосредственно в киберпространстве (кража персональных данных, нарушение прав интеллектуальной собственности, распространение вредоносного программного обеспечения); 3) преступления, связанные с незаконным хранением нелегальной информации, сведений о преступной деятельности и проч.⁵ Критерии классификации, сформулированные указанными авторами, подкрепляют нашу позицию о разнообразности собственно киберправонарушений и правонарушений информационного характера, не позволяя согласиться с мнением авторов, отождествляющих эти группы уголовных правонарушений⁶.

Итак, обозначенная *первая группа* собственно киберправонарушений объединяет нормы об ответственности за правонарушения, объектом которых является информационная безопасность и информационный суверенитет личности, общества и государства, а предметом (способом и(или) средством) — информация, цифровые технологии, компьютерные системы, программное обеспечение, объекты информационной инфраструктуры, специальные технические

¹ См., например: Полякова Т. А., Минбалиев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. 2019. № 3 (33). С. 64—68. DOI: 10.14529/securl90307; Рахмон Д. С. Некоторые вопросы, связанные с правовой защитой национальных интересов и национальной безопасности в условиях глобальных вызовов и угроз // Правовая жизнь. 2019. № 3 (27). С. 11; Расулев А. Концептуальные основы уголовно-правовой охраны информационных отношений в Республике Узбекистан // Правосудие (Одил судлов). 2019. № 1. С. 94.

² Модель двучленной классификации обосновывалась авторами в более ранних исследованиях. См., например: Семькина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6 (61). С. 105, 111. DOI: 10.12737/23525; Ключко Р. Н. Проблемы уголовно-правового воздействия за действия информационного характера // Проблемы эффективности осуществления правоохранительной функции в обеспечении социально-экономической стабильности в обществе: сб. матер. Междунар. науч.-практ. конф. Минск, 2018. 9—10 нояб. / под ред. В. В. Марчука, А. В. Солтановича. Минск, 2018. С. 61—65.

³ См.: Артемов В. Ю., Власов И. С., Голованова Н. А. и др. Новые направления развития уголовного законодательства в зарубежных государствах: сравнительно-правовое исследование: монография / отв. ред. Н. А. Голованова, С. П. Кубанцев. М., 2019. С. 223—226; Голованова Н. А. Уголовное право Англии: учеб. пособие для бакалавриата и магистратуры. М., 2017. С. 144—148.

⁴ См. также: Власов И. С., Голованова Н. А., Меньших А. А. Ответственность за компьютерные преступления по законодательству зарубежных государств // Журнал зарубежного законодательства и сравнительного правоведения. 2005. № 2. С. 122—123.

⁵ См.: Артемов В. Ю., Власов И. С., Голованова Н. А. и др. Указ. соч. С. 229—230.

⁶ См., например: Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex russica. 2018. № 4. С. 108. DOI: 10.17803/1729-5920.2018.137.4.108-120.

средства. В эту группу входят, например, несанкционированный доступ к компьютерной информации, модификация такой информации и незаконное завладение ею, компьютерный саботаж, незаконный оборот вредоносных компьютерных программ и продуктов, неправомерное распространение электронных информационных ресурсов с ограниченным доступом, получение неправомерного доступа к информации с использованием специальных технических средств.

«Эталонная» система собственно киберправонарушений сформирована в гл. 30 Особенной части Модельного Уголовного кодекса от 17 февраля 1996 г.⁷ (далее — Модельный УК). Во многом (но, как покажет дальнейшее изложение, не в абсолютном большинстве случаев) этот критерий послужил «фундаментом» криминализации собственно киберправонарушений в особенных частях уголовных кодексов государств — участников СНГ, а именно: в гл. 28 «Преступления в сфере компьютерной информации» (ст. 272—274¹) УК РФ 1996 г.; в гл. 30 «Киберпреступления» (ст. 272—273) УК Азербайджана 1999 г.; в гл. 24 «Преступления против безопасности компьютерной информации» (ст. 251—257) УК Армении 2003 г.; в гл. 31 «Преступления против информационной безопасности» (ст. 349—355) УК Республики Беларусь 1999 г.; в гл. 7 «Уголовные правонарушения в сфере информатизации и связи» (ст. 205—213) УК Казахстана 2014 г.; в гл. XI (ст. 259—261-1) «Информационные преступления и преступления в области электросвязи» УК Молдовы 2002 г.; в гл. 42 «Преступления против информационной безопасности» (ст. 304—306) УК Кыргызстана 2017 г. и в гл. 29 «Проступки против информационной безопасности» (ст. 159—160) Кодекса Кыргызстана о проступках 2017 г. (далее — КоП Кыргызстана); в гл. 28 «Преступления против информационной безопасности» (ст. 298—304) УК Таджикистана 1998 г.; в гл. 33 «Преступления в сфере информатики и связи» (ст. 333—335.3) УК Туркменистана 1997 г.; в гл. XX-1 «Преступления в сфере информационных технологий» (ст. 278-1—278-7) УК Узбекистана 1994 г.

Компаративный обзор приведенных глав уголовных кодексов государств — участников СНГ и норм, в них содержащихся, позволил выявить некоторые закономерности. Одна из них отражает тождество подходов большего числа УК к признанию в качестве родового (видового) объекта собственно киберправонарушений обеспечения состояния защищенности информационной безопасности компьютерной

информации, информационных и телекоммуникационных систем. И это не случайно, поскольку такая унифицированная модель объекта уголовно-правовой охраны предложена в Модельном УК, которым руководствовались законодатели при разработке уголовных кодексов России⁸, Азербайджана, Армении, Беларуси, Кыргызстана и Таджикистана.

Но интенсивная цифровая трансформация изменила прежнюю наполняемость информационной безопасности. Для современного понимания существа этого объекта уголовно-правовой охраны следует учитывать, что совокупность общественных отношений в сфере информационной безопасности образует «суперинститут» информационного права и давно не исчерпывается традиционным пониманием безопасности компьютерной информации, информационных и телекоммуникационных систем. Состав этого «суперинститута» формируют несколько сходных по целевому назначению институтов: безопасности информационных ресурсов, информационного суверенитета, информационно-телекоммуникационных технологий, сетей связи и защиты информации ограниченного доступа⁹.

С этих позиций мы солидарны с научным подходом¹⁰ широкого понимания информационной безопасности как состояния защищенности информации, содержащейся в компьютерной системе или передаваемой с помощью сетевых информационных технологий, специальных технических средств и сетей связи, от неправомерного ее использования самими ИТ-разработчиками, субъектами — собственниками цифровых технологий либо иными потребителями информационно-телекоммуникационных систем. Сегодня информационная безопасность, во-первых, является неотъемлемым элементом информационных отношений, во-вторых, сопряжена с обеспечением информационного суверенитета личности, общества и государства, в-третьих, выступает дополнительным объектом всех преступлений информационного характера, совершаемых посредством цифрового и информационно-телекоммуникационного воздействия. Такая интерпретация информаци-

⁸ См., например: Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / отв. ред. В. М. Лебедев. М., 2017. Т. 3: Особенная часть. Раздел IX.

⁹ Подробнее см.: Бачило И. Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства: сб. науч. работ / отв. ред. И. Л. Бачило. М., 2015. С. 7—12.

¹⁰ См., например: Юсупов Р. М., Бачило И. Л., Бондуровский В. В., Вус М. А., Макаров О. С. Правовой вектор обеспечения информационной безопасности в модельном законодательстве СНГ // Диалог: политика, право, экономика. 2017. № 2 (5). С. 50—51; Шаухаров К. Уголовные правонарушения в сфере информатизации и связи // Заңгер — Вестник права Республики Казахстан. 2017. № 3 (188). С. 43—48.

⁷ В ред. постановления МПА СНГ от 27 ноября 2015 г. № 43-16 «Изменения в Модельный Уголовный кодекс для государств — участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере». URL: https://iacis.ru/upload/iblock/5a0/prilozhenie_k_postanovleniyu_43_16.pdf.

онной безопасности, на наш взгляд, подчеркивает целесообразность коррекции положений и Модельного УК, и уголовных кодексов некоторых государств — участников СНГ (в том числе уголовные кодексы России и Беларуси) относительно определения родового (видового) объекта собственно киберправонарушений. В связи с тем что угрозы информационной безопасности возникают в разных сферах жизнедеятельности личности (имущественной, экономической, интимной), общества (нравственности и здоровья населения) и государства (конституционного строя, мира и безопасности человечества), вариантом родового (видового) объекта собственно киберправонарушений может стать более узкая, входящая в «суперинститут» информационной безопасности сфера — информатизации и связи. Сходный широкий подход уже имеет место в уголовных кодексах Казахстана, Молдовы и Узбекистана.

Другая закономерность касается отклонений от «эталонного» потенциала Модельного УК, точнее, характеризуется множеством расхождений подходов Модельного УК и уголовных кодексов государств — участников СНГ к содержанию отдельных составов собственно киберправонарушений. Так, исходя из компаративного анализа системы и конструкции норм, включенных в соответствующие главы уголовных законов, можно дифференцировать две модели криминализации собственно киберправонарушений: а) «усеченную» (иллюстрируемую группой посягательств в гл. 28 УК РФ и системой уголовных правонарушений в кыргызском уголовном законодательстве, объединяющей преступления гл. 42 УК Кыргызстана, и уголовных проступков гл. 29 КоП Кыргызстана); б) «расширенную» (максимально приближенную к структуре гл. 30 Модельного УК и характерную для уголовных кодексов иных государств — участников СНГ)¹¹.

Например, в сопоставлении с гл. 28 УК РФ наполняемость (не только количественная, но и качественная) сходных глав Модельного УК и уголовных кодексов других государств — участников СНГ не идентична. Во-первых, в системе собственно киберправонарушений, сформированной в уголовных кодексах некоторых стран, можно встретить деяния, не криминализованные в УК РФ и не имеющие «эталонной» нормы в Модельном УК, например так называемый хостинг. Хостинг, понимаемый как оказание провайдером услуг по предоставлению (размещению) интернет-ресурсов в противоправных целях, включен в число собственно киберправонарушений в УК Казахстана (ст. 212) и УК Туркменистана (ст. 335).

¹¹ См.: Дубко М. А. Неправомерное завладение компьютерной информацией как преступление против информационной безопасности: автореф. дис. ... канд. юрид. наук. Минск, 2018. С. 10—11.

Во-вторых, уголовные кодексы всех государств — участников СНГ криминализируют незаконный оборот специальных технических средств, предназначенных для негласного получения информации, но не везде данное посягательство наделено свойственной ему юридической природой собственно киберправонарушения. В Модельном УК (ст. 290), уголовных кодексах Азербайджана (ст. 273.1), Армении (ст. 255), Республики Беларусь (ст. 353), Таджикистана (ст. 302) и Узбекистана (ст. 278-3) это деяние обоснованно квалифицируется как собственно киберправонарушение, посягающее на информационный суверенитет личности, общества и государства. В уголовных кодексах Кыргызстана (ст. 252) и Молдовы (ст. 301-1) прописан более широкий подход, в котором определен родовый (видовой) объект незаконного оборота специальных технических средств, создающего угрозу общественной безопасности и общественному порядку, поглощающий своим содержанием и информационную безопасность, и информационный суверенитет. В широком контексте посягательства на основы конституционного строя и безопасности государства трактует это деяние и УК Туркменистана (ч. (1), (3) ст. 179). Для сравнения: УК РФ (ст. 138¹) значительно сузил сферу уголовно-правовой охраны и при защите от данного деяния отдал приоритет конституционным правам и свободам человека и гражданина.

В-третьих, в уголовных кодексах государств — участников СНГ встречаются составы, хотя и включенные в гл. 28 УК РФ, но формулирующие другие криминообразующие признаки. Сравним подходы к установлению ответственности за незаконный оборот специальных технических средств или программных продуктов, изготовленных, разработанных или адаптированных для целей совершения преступлений, сопряженных с использованием цифровых технологий, закрытый перечень которых определен в диспозиции соответствующей статьи УК. Компаративный рубрикатор позволяет выделить три подхода к криминализации этого киберправонарушения:

а) кумулятивный, при котором ответственность активируется не только за неправомерный оборот соответствующих технических средств или программных продуктов для совершения правонарушений против информационной безопасности (предусмотренных этой же главой УК), но и для целей иных правонарушений («растворенных» в других главах Особенной части), совершаемых «цифровым» способом. Например, в диспозиции ст. 259, 260 УК Молдовы указаны как собственно киберправонарушения (несанкционированный доступ к компьютерной информации, неправомерный перехват данных, нарушение целостности информационных данных, воздействие на функционирование информационной системы, подлог информационных данных, инфор-

мационное мошенничество), так и преступления информационного характера (изготовление или сбыт поддельных кредитных карт либо платежных документов);

б) сингулярный, когда в отличие от предыдущего подхода криминообразующим признаком производства устройств или компьютерных программ признано их изготовление или адаптация только в целях совершения одной группы деяний — собственно киберправонарушений. Так, в ст. 273-1 УК Азербайджана установлена ответственность за оборот средств, предназначенных для неправомерного доступа к компьютерной информации; неправомерного завладения компьютерной информацией; неправомерного вмешательства в компьютерную систему или компьютерную информацию;

в) гибридный, при котором изготовление или сбыт специальных технических средств как правонарушения против информационной безопасности предназначены для совершения лишь одного деяния с тождественным родовым (видовым) объектом — несанкционированного доступа к компьютерной информации (ст. 255 УК Армении, ст. 353 УК Республики Беларусь, ст. 302 УК Таджикистана, ст. 278-2 УК Узбекистана). Дополнительно незаконные изготовление, разработка, использование и продажа каких-либо специальных технических средств могут включаться в качестве криминообразующего признака составов других правонарушений, с иным родовым (видовым) объектом. Например, в УК Беларуси изготовление или сбыт поддельных платежных средств, включая пластиковые карты, является преступлением в сфере экономической деятельности (ст. 222).

Различия в подходах к определению криминообразующих признаков выявляются при имплементации в уголовных кодексах государств — участников СНГ положений ст. 289 Модельного УК в части: а) несанкционированного завладения компьютерной информацией (ее несанкционированного копирования либо получения иным способом), хранящейся в компьютерной системе, сети или на машинных носителях, и(или) перехвата информации, передаваемой с использованием средств компьютерной связи; б) принуждения к передаче компьютерной информации путем шантажа лица, в ведении или под охраной которого такая информация находится, либо его близких, или под угрозой уничтожения или повреждения имущества этих лиц, либо применения к ним физического насилия. В уголовных кодексах одних государств, например в ст. 272 УК Азербайджана, предусмотрена ответственность лишь за завладение (без конкретизации такого способа, как перехват) неправомерным лицом с использованием технических средств компьютерной информацией, не предназначенной для общего доступа либо содержащейся в компьютерной системе (ее части) инфраструктурного объекта общественного значения. Аналогичные предметы

посягательства и способы неправомерного завладения определены в ст. 208 УК Казахстана. В статье 352 УК Беларуси под неправомерным завладением информацией понимаются повлекшие причинение существенного вреда несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а также перехват информации, передаваемой с использованием средств компьютерной связи. В уголовных кодексах других стран, в частности в ст. 254 УК Армении, кроме неправомерного завладения компьютерной информацией и ее перехвата, криминализировано также принуждение к ее передаче лицом, в ведении или под охраной которого такая информация находится, или его близкими. Безусловно, изложенный перечень отличий в подходах к регламентации неправомерного завладения компьютерной информацией в Модельном УК и уголовных кодексах государств — участников СНГ не является исчерпывающим¹².

В целом при всей позитивной оценке современного состояния системы собственно киберправонарушений проведенный компаративный обзор позволяет солидаризироваться с мнением белорусского исследователя М. А. Дубко о незавершенности этапа определения правовых мер противодействия таким деяниям. Для обеспечения корреспонденции норм уголовных законов с системой дозволений, запретов, ограничений и стимулов, формирующих правовой режим в информационной сфере, актуально принятие самостоятельного нормативного правового акта¹³, который (например, по аналогии с антикоррупционным правовым регулированием¹⁴) составит ядро нормативной базы. Возможно, такой силой будет обладать отдельный закон о противодействии преступлениям в сфере информатизации и связи или кодекс об информационной безопасности, концентрирующий наряду с общими вопросами универсальные и региональные международные стандарты о правовом режиме оборота цифровой информации. Для государств — участников СНГ «пруденциальным» нормативом в этой сфере правового регулирования мо-

¹² См., например: Дубко М. А. Совершенствование уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией (ст. 352 УК) // Вестник Академии МВД Республики Беларусь. 2018. № 1 (35). С. 133—134.

¹³ См.: Дубко М. А. Основание и причины криминализации неправомерного завладения компьютерной информацией // Вестник Академии МВД Республики Беларусь. 2017. № 1 (33). С. 88.

¹⁴ См., например: Хабриева Т. Я., Андриченко Л. В., Цирин А. М. и др. Организационно-правовые механизмы противодействия коррупции в субъектах Российской Федерации: монография. М., 2019. С. 27. DOI 10.31085/9785392288113-2019-224.

гут стать разработанные Межпарламентской ассамблеей (МПА) СНГ вводимые в действие в ближайшей перспективе Модельный закон «О пресечении нарушений в области информационно-коммуникационных технологий (ИКТ)» и Рекомендательные типологии новых преступлений, совершаемых с использованием цифровых технологий¹⁵.

Вторую группу уголовных правонарушений составляют деяния информационного характера, сопряженные с информационно-телекоммуникационным воздействием, в которых «цифровой» способ и (или) предмет в электронной форме являются одним из криминообразующих признаков состава посягательства (иными словами, отражают его направленность), а информационная безопасность и (или) информационный суверенитет рассматриваются как дополнительные объекты посягательства. Нередко наступление общественно опасных последствий от совершения таких правонарушений может проявиться лишь в отдаленном будущем, не всегда они (последствия) имеют количественные характеристики в виде размера вреда, но угрозы от них охраняемым объектам могут быть футурологически значимы до такой степени, что определяют необходимость своевременной реакции уголовного закона.

В государствах — участниках СНГ наблюдаются неодинаковые подходы к криминализации правонарушений информационного характера, являющихся разнообъектными и посягающих на различные сферы общественных отношений (личность, собственность, экономику, здоровье населения, общественную нравственность, безопасность государства). Видовой состав уголовных правонарушений подобного рода экстравертен и постоянно обновляется. Прежде всего под воздействием гармонизации законодательства государств — участников СНГ пересматриваются уголовно-правовые механизмы по предотвращению использования сетевых технологий и иного информационно-телекоммуникационного воздействия для целей терроризма и насильственного экстремизма, ведущего к терроризму. В установках межпарламентских экспертных обсуждений¹⁶ и в регуляторной политике МПА СНГ¹⁷ озвучены такие приоритеты криминализации, как пропаганда в молодеж-

ной среде деструктивной идеологии в сети Интернет, вербовка через сетевые ресурсы для участия в боевых действиях в зонах вооруженных конфликтов, оказание IT-помощи террористам, диверсионная террористическая и экстремистская деятельность в киберпространстве. По сути, речь идет о запуске механизмов уголовно-правовой блокировки одной из общественно опасных технологий «цифрового» противостояния — информационно-психологической агрессии и информационно-психологической войны в целях нанесения ущерба национальным интересам и национальной безопасности в мирных условиях¹⁸.

О срочной необходимости введения ответственности за совершение перечисленных деяний также сигнализируют экспертные оценки центрального органа отраслевого сотрудничества СНГ в сфере противодействия террористическим угрозам и вызовам — Антитеррористического центра государств — участников СНГ (АТЦ СНГ). Эксперты АТЦ СНГ среди новейших факторов, определяющих террористические угрозы на платформе СНГ, называют информационно-пропагандистскую и вербовочную деятельность международных террористических и религиозных экстремистских организаций в киберпространстве, сконцентрированную на ведении дестабилизирующей работы в государствах — участниках СНГ. Эпоха цифровизации не только расширила преступную практику онлайн-вербовки наемников для участия в боевых действиях, но и облегчила активацию технологии «спящих ячеек»¹⁹. Особенно активно в распространении в государствах — участниках СНГ деструктивных материалов через интернет-ресурсы, социальные сети и мессенджеры участвуют проигиловские группировки хакеров, образующие так называемый Объединенный киберхалифат (United Cyber Caliphate)²⁰.

Принимая во внимание экспертно-рейтинговые оценки, можно заключить, что в уголовных кодексах многих государств — участников СНГ в сфере противодействия терроризму и насильственному экстремизму, в том числе совершаемым с использованием сетевых технологий, уже сформирована опытная нормативная правовая база. В недавно обнародованном исследовании «Глобальный индекс терроризма

¹⁵ URL: https://iacis.ru/pressroom/news/komissii_mpa_sng/v_tavrisheskom_dvortse_proshlo_zasedanie_obedinennoy_komissii_pri_mpa_sng_po_garmonizatsii_zakonodatelstva_v_sfere_bezопасности_i_protivodeystviya_nov/.

¹⁶ См., например: Выводы организаторов Конференции по противодействию международному терроризму, организованной МПА СНГ (18 апреля 2019 г., г. Санкт-Петербург). URL: <https://iacis.ru/upload/medialibrary/4fd/vyvody-organizatorov-konferentsii.pdf>.

¹⁷ См., например, Программу сотрудничества государств — участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2020—2022 го-

ды (утв. Решением Совета глав государств СНГ от 11 октября 2019 г.).

¹⁸ Подробнее см.: Шубаев Д. В. Методы противодействия информационной войне // Российский журнал правовых исследований. 2016. № 4 (9). С. 60—68. DOI: <https://doi.org/10.17816/RJLS18192>. URL: <https://journals.eco-vector.com/2410-7522/article/view/18192>.

¹⁹ См.: Сухаренко А. Н. Антитеррористическое сотрудничество государств СНГ: состояние и тенденции // Диалог: политика, право, экономика. 2018. № 4 (11). С. 38.

²⁰ Подробнее см.: Профилактика терроризма и экстремизма в молодежной среде. СПб., 2018. С. 9, 14, 39.

2019» (Global Terrorism Index — GTI) самыми безопасными от угрозы терроризма на пространстве интеграционного объединения СНГ признаны Беларусь и Туркменистан²¹. В рейтинге GTI 2019 г. эти страны заняли последнее место (из 138 возможных рейтинговых позиций). Среди государств — участников СНГ отмечены улучшения безопасности от террористических атак у Узбекистана (135-е место), Молдовы (123-е), Азербайджана (103-е), Армении (94-е), Казахстана (85-е) и Российской Федерации (37-е место). В рейтинге GTI 2019 г. «очень низкий уровень» опасности указан в Узбекистане, Молдове, Азербайджане, Армении и Казахстане, «низкий» — в Таджикистане (хотя и ухудшившем свои позиции до 50-го места), «средний» — в Российской Федерации²².

Частично обосновать такую ситуацию с ранжированием «термометра» безопасности среди государств — участников СНГ можно посредством компаративного обзора. В юрисдикциях всех государств — участников СНГ криминализированы пропаганда террористической и экстремистской деятельности, призывы к нарушению национальной безопасности государства и разжиганию межнациональной розни, осуществляемые посредством цифровых коммуникаций. Например, в отличие от ст. 169.1 УК Туркменистана далеко не во всех уголовных кодексах государств — участников СНГ криминализированы вербовка через сетевые ресурсы для участия в боевых действиях в зонах вооруженных конфликтов и оказание IT-помощи террористам. Ответственность за заведомое оказание информационно-телекоммуникационных услуг физическим и юридическим лицам для финансирования террористической и экстремистской деятельности введена в ст. 258 УК Казахстана и ст. 177.2 УК Туркменистана. УК Молдовы (ст. 279 во взаимосвязи со ст. 132-1) и Таджикистана (ст. 179(2)) в предмет финансирования терроризма включили документы и иные юридические инструменты в электронной и цифровой форме, подтверждающие право на любого рода финансовые ценности (активы).

Однако в уголовных кодексах некоторых государств — участников СНГ все еще отсутствуют критерии криминализации публичного информационно-воздействия в целях распространения и оправдания деструктивной идеологии. УК Беларуси, например, не дифференцирует этот относительно новый для мировой практики манипулятивный способ совершения преступлений террористической и экстремистской направленности²³. Для сравнения: УК РФ

признал общественную опасность публичного оправдания деструктивной идеологии терроризма (ст. 205²) и нацизма (ст. 354¹). Превенцией от неограниченного распространения деструктивных идей религиозного экстремизма цифровым способом обладает ст. 167-2 УК Азербайджана об ответственности за незаконное производство, ввоз, продажу или распространение литературы в электронном формате, аудио- и видеоматериалов религиозного содержания, товаров и изделий религиозного назначения. Во многом сходная норма включена в ст. 244-1 УК Узбекистана.

В группу уголовных правонарушений информационного характера входит также ряд иных деяний, в составах которых «цифровой» признак является криминообразующим. Например, с каждым днем все больше юрисдикций государств — участников СНГ признают общественную опасность онлайн-хищений. Однако, как и в рассмотренных выше примерах, в Модельном УК и уголовных кодексах государств — участников СНГ нет одинакового подхода к криминализации «цифрового» признака в составах таких посягательств на чужое имущество.

Наиболее распространена модель включения неправомерного использования «цифрового» признака в качестве отягчающих обстоятельств «традиционных» форм хищения. Но даже в этом, на первый взгляд одинаковом, воплощении идеи криминализации «цифрового» признака компаративный обзор позволил подчеркнуть некоторые различия. Одна группа состоит в неодинаковом конъюнктурном подходе — выборе в УК конкретной формы хищения, требующей усиленной криминализации в случае наличия в ее составе «цифрового» признака. Например, в уголовных кодексах России и Казахстана этот признак является обстоятельством, отягчающим наказание за две формы хищения — кражу и мошенничество. В УК Узбекистана криминализированы три формы хищнического завладения чужим имуществом с использованием информационно-телекоммуникационных технологий — кража, мошенничество, присвоение или растрата. Упоминание об одной форме хищения содержится в уголовных кодексах Азербайджана (кража) и Молдовы (мошенничество). В отличие от этих примеров УК Беларуси не «умножает» квалифицирующие признаки в известных науке и практике традиционных формах хищения, а выделяет их в специальную форму, рассчитанную на ситуации, когда хищение имущества про-

²¹ См.: URL: <https://rg.ru/2019/11/20/belarus-i-turkmenistan-priznali-samymi-bezopasnymi-stranami-sng.html>.

²² См.: Global Terrorism Index 2019: Measuring the Impact of Terrorism. Sydney, 2019. P. 8—9. URL: <http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf>.

²³ Подробнее см.: Ключко Р. Н. Общественно опасное информационное воздействие: виды и особенности уголовно-

правовой оценки // Безопасность и устойчивое развитие: теория и практика в условиях цифровой трансформации: матер. Междунар. науч.-практ. конф. Минск, 5—6 декабря 2019 г.: в 5 т. / редкол.: Г. Г. Краско (гл. ред.) и др. Минск, 2019. Т. 3. С. 59—60; Макаров О. С., Баныковский А. Л. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь. URL: <https://zakonrb.com/npa/makarov-os-bankovskiy-al-konceptualnye-napravleniya>.

изводится исключительно с помощью электронной техники²⁴.

Другая группа отличий не столько характеризует выбор законодателя в определении объекта посягательства (наделение онлайн-хищения «окраской» имущественного деяния или отождествление его объекта с обеспечением информационной безопасности), сколько заключается в определении юридического свойства самого «цифрового» признака (признание его способом совершения уголовного правонарушения с особым предметом «оцифрованного» (нематериального) характера). Например, в апреле 2018 г.²⁵ УК РФ установил общественную опасность хищения предметов путем информационно-телекоммуникационного воздействия на обремененную в цифровую форму конфиденциальную информацию о платежных активах. В результате в п. «г» ч. 3 ст. 158 обосновалось новое, особо квалифицирующее обстоятельство — кража, совершенная с банковского счета, а равно в отношении электронных денежных средств, а в ст. 159³ расширен способ мошенничества — от использования платежных карт до электронных систем платежа. Но при этом УК РФ в системе преступлений против собственности сохранил введенную еще в ноябре 2012 г. ответственность за мошенничество в сфере компьютерной информации (ст. 159⁶), где «цифровой» признак отождествляется со способом информационно-телекоммуникационного воздействия на функционирование электронных носителей информации в целях безвозмездного изъятия и (или) обращения в пользу виновного компьютерной информации.

В науке российского уголовного права²⁶ приведенный подход к формулированию «цифрового» признака хищений подобным казуистичным образом вызвал критические замечания. Дискуссионные суждения о правовой неопределенности породило юридико-техническое «оцифрование» криминообразующих признаков кражи и специальных видов мошенничества путем использования в их конструкциях словарных оборотов различных с точки зрения лексики, но, по сути, идентичных с позиции этимологии. В частности, у правоприменителя могут возникнуть трудности при отграничении как минимум четырех деяний: кражи с банковского счета и в отношении электронных денежных средств (п. «г» ч. 3 ст. 158

УК РФ), мошенничества с использованием электронных средств платежа (ст. 159³ УК РФ), мошенничества в сфере компьютерной информации (ст. 159⁶ УК РФ) и даже «классического» мошенничества (ст. 159 УК РФ), совершаемого путем распространения заведомо ложных сведений в интернет-ресурсах. При квалификации «цифровых» хищений возможны и иные вопросы, например: требует ли дополнительной квалификации по ст. 272 УК РФ (относимой к группе собственно киберправонарушений) совершение мошенничества в сфере компьютерной информации путем неправомерного доступа к компьютерной информации?

Казалось бы, с одной стороны, постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» приводит обобщающие рекомендации о разрешении этих квалификационных дилемм. Так, разъяснено, что при отсутствии незаконного воздействия виновного на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети хищение путем использования учетных данных собственника (иного владельца) имущества независимо от способа получения к ним доступа надлежит квалифицировать как кражу (абз. 1 п. 21). Сопряженность же мошенничества в сфере компьютерной информации с неправомерным доступом к компьютерной информации либо с созданием, использованием и распространением вредоносных программ помимо ст. 159⁶ УК РФ требует дополнительной квалификации по статьям о преступлениях в сфере компьютерной информации (ст. 272, 273 или 274¹ УК РФ) (абз. 2 п. 20). Не образует мошенничества в сфере компьютерной информации и квалифицируется как «классическое» мошенничество хищение чужого имущества или приобретение права на чужое имущество, совершенное посредством распространения заведомо ложных сведений в информационно-телекоммуникационных сетях (абз. 2 п. 21).

Однако изменения, появившиеся в п. «г» ч. 3 ст. 158 и ст. 159³ УК РФ в апреле 2018 г., заставляют сомневаться в отмеченной наукой практической ценности приведенных в названном постановлении основ квалификации специальных видов мошенничества²⁷. Появление этих составов позволяет высказывать предположение о появлении в практике случаев смешения хищения с использованием цифровых и информационно-телекоммуникационных технологий в форме кражи и отдельных видов мошенничества как посягательства на собственность с самостоятельным видом компьютерного хищения, предметом которого является электронная информация, а спо-

²⁴ См., например: Уголовный кодекс Республики Беларусь: науч.-практ. коммент. / под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. Минск, 2019. С. 458—461.

²⁵ См. Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

²⁶ См., например: Русскиевич Е. А. Отграничение кражи с банковского счета или в отношении электронных денежных средств от смежных составов преступлений // Уголовное право. 2019. № 2. С. 59—64.

²⁷ См.: Кибальник А. Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда РФ // Уголовное право. 2018. № 1. С. 61—67.

собом ее получения — информационно-телекоммуникационное воздействие. Это предположение основано на опыте легитимации «цифровых» хищений в Модельном УК и в близких к УК РФ по правовым традициям уголовных кодексах Армении, Молдовы и Беларуси. Например, предметом информационного мошенничества, закрепленного в ст. 260-6 УК Молдовы, является не чужое имущество в его общеизвестном материальном понимании, а электронная информация о нем, полученная, обрабатываемая и хранящаяся в компьютерной сети или информационной системе, на цифровых носителях либо в базе данных других технических средств информационной системы или сети. При этом, несмотря на признание в УК Молдовы родовым объектом онлайн-мошенничества информационной безопасности компьютерных систем, обязательный признак субъективной стороны ст. 260-6 имеет направленность имущественного посягательства, поскольку состоит в цели содействия в завладении материальным предметом и (или) реальной выгодой²⁸.

Иная модель криминализации хищения чужого имущества с использованием компьютерных технологий представлена в ст. 243 Модельного УК, ст. 181 УК Армении и ст. 212 УК Республики Беларусь. Речь идет об отдельном виде посягательства на собственность, специальной форме хищения, не являющихся частными случаями кражи, мошенничества, присвоения или растраты, когда имущество изымается и обращается в пользу виновного или других лиц не путем воздействия на личность (человека), а исключительно с помощью информационно-телекоммуникационного воздействия на электронные идентификационные сведения о предмете деяния. Например, в обобщающих рекомендациях Пленума Верховного суда Республики Беларусь разъясняется, что хищение с использованием компьютерной техники, предусмотренное ст. 212 УК, заключается в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находится, с использованием системы обработки информации. Такое хищение может совершаться как путем изменения электронной информации (обрабатываемой в компьютерной системе, хранящейся на цифровых носителях или передаваемой по сетям передачи данных), так и по-

средством введения в компьютерную систему ложной информации²⁹.

Белорусские ученые и практики конкретизируют³⁰, что на квалификацию хищений, совершаемых с использованием этой техники, влияет не само использование компьютерной техники или ее комплектующих элементов (поскольку таковое расценивается как средство совершения хищения), а информационно-телекоммуникационное воздействие на результат автоматизированной обработки сведений об имуществе в целях завладения ими. В компьютерной системе хранится не материальный предмет преступления, а информация о нем и его передвижении — денежных средствах, имуществе либо иных вещах, на которые осуществляется посягательство. Таким образом, юридическая сущность хищения с использованием цифровых возможностей компьютерной техники выражается в модификации автоматизированных данных путем информационно-телекоммуникационного воздействия виновного не на человека, а на информацию об имуществе, содержащуюся в сетевых ресурсах, и видоизменении такой информации в части перехода имущества от собственника либо законного владельца к иному лицу. Компьютерная техника, таким образом, является не предметом хищения, а «цифровым оружием» совершения этого деяния³¹.

Хищение с использованием компьютерной техники возможно лишь путем компьютерных манипуляций (перехвата информации; несанкционированного доступа к источникам информации; вмешательства в компьютерную систему посредством ввода, изменения, удаления, фальсификации или блокирования данных). В отличие от кражи и мошенничества незаконное завладение чужим имуществом с помощью электронной техники производит не сам преступник. Для его санкционирования используется электронное устройство, идентифицирующее виновного как собственника (законного владельца) в связи с внесенными им изменениями в автоматизированную компьютерную систему. Если первоначально компьютерная техника использовалась для изготовления фиктивных документов, и только затем полученный фальсификат применялся для завладения чужим имуществом путем обмана, все содеянное охватывается рамками мошенничества. Случаи, когда хищение, сопровождающееся несанкционированным доступом к автоматизированной информации, повлекло по неосторожности

²⁸ Подробнее см.: Семькина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6 (61). С. 105—111. DOI: 10.12737/23525; Семькина О. И. Актуализация ответственности за хищения с использованием кибертехнологий в свете экономических угроз: опыт регламентации в законодательстве зарубежных государств // Электронная валюта в свете современных правовых и экономических вызовов: сб. матер. междунар. науч.-практ. конф. (2 июня 2016 г.) / редкол.: А. С. Генкин, Э. Л. Сидоренко, О. И. Семькина. М., 2016. С. 449—452.

²⁹ См. абз. 1 п. 20 постановления Пленума Верховного суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества».

³⁰ См., например: Уголовный кодекс Республики Беларусь: науч.-практ. коммент. / под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. С. 459.

³¹ Там же. С. 458—459.

нарушение систем защиты, крушение, аварию, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, требуют дополнительной квалификации по ч. 2 или 3 ст. 349 УК Беларуси (несанкционированный доступ к компьютерной информации). Модификация компьютерной информации в целях извлечения материальных выгод, например осуществление мобильных разговоров за чужой счет путем «клонирования» телефонных сим-карт, образует самостоятельный способ причинения имущественного ущерба без признаков хищения, ответственность за который установлена в ст. 216 УК Беларуси³².

Сравнив киберпространство с «неконтролируемой общественной игровой площадкой», где недобросовестные субъекты порой безнаказанно «могут преследовать, запугивать и порочить других, вызывая эмоциональный и психологический стресс»³³, кроме раскрытых выше можно также обозначить иные тренды конструирования механизмов «жесткого права». Уже не носит прогнозного характера тот факт, что категориальный аппарат действующих сегодня УК не всегда будет идти в ногу с завтрашним днем, наступление которого явит обществу новые цифровые технологии, терминологию и альтернативные физическим виртуальные способы совершения преступлений. К тому же общественная опасность преступлений, содержащих «цифровой» признак, может выражаться не только в причинении или угрозе причинения вреда охраняемым уголовным законом объектам, но и в направлении такого воздействия на воспроизведение преступности. Поэтому важно своевременно пресечь прогрессирующую преступную изобретательность в применении цифровых технологий и как можно скорее создать фундамент для внедрения не просто новаторских, а соответствующих современной практике механизмов противодействия цифровому произволу³⁴.

³² См. также: п. 21, 22 постановления Пленума Верховного суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества»; Уголовный кодекс Республики Беларусь: науч.-практ. коммент. / под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. С. 460—461, 468—471, 772—776.

³³ Голованова Н. А. Новые формы онлайн-преступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 43—46. DOI: 10.12737/jfcl.2019.3.4.

³⁴ Подробнее см.: Ключко Р. Н. Информационное воздействие: потенциальные угрозы и проблемы уголовно-правовой оценки // Оптимизация правовой основы противодействия преступности: к 25-летию Конституции Российской Федерации: сб. науч. трудов по итогам Всерос. науч.-практ. конф. с междунар. участием, г. Волгоград, 12—13 декабря 2018 г.: в 2 ч. Ч. 1 / под ред. Л. В. Лобановой, С. М. Мкртчян; редкол.: Л. В. Лобанова (отв. ред.) и др. Волгоград, 2018. С. 93—98.

К разрушительным последствиям для национальной безопасности может привести запоздалая реакция уголовного закона на необходимость установления и (или) усиления запретов использования цифровых технологий для деструктивного информационного воздействия на подрастающее поколение, публичного содействия девиантности молодежи³⁵. В государствах — участниках СНГ наметилась тенденция к усилению ответственности за применение цифровых технологий в преступлениях против несовершеннолетних. Например, еще в 2012 г. в УК Молдовы была введена ст. 175-1 об осуществлении с использованием информационных технологий либо средств электронных коммуникаций обольщения несовершеннолетних с целью совершения в отношении них половых преступлений посредством предложения, убеждения, манипулирования, угрозы и любых обещаний выгод. В УК Армении охрана половой неприкосновенности несовершеннолетних усилена путем криминализации непристойных действий с применением сетей электронной связи (п. 6 ч. 2 ст. 142). УК Казахстана установил ответственность за вовлечение несовершеннолетних в преступную деятельность (ч. 2—4 ст. 132) или в занятие проституцией (п. 1.1 ч. 3, ч. 4 ст. 134) посредством использования сети Интернет. Приведенные примеры криминализации могут стать опытной базой для реализации в УК РФ тех установок Концепции информационной безопасности детей в Российской Федерации³⁶, которые ориентированы на формирование новых запретов деструктивного информационного воздействия на молодежь.

Высокой степенью общественной опасности обладают вредоносные информационно-телекоммуникационные воздействия на нематериальные объекты уголовно-правовой охраны, представляющие угрозу для личности, общества и государства. Острота ситуации заключается в том, что довольно сложно просчитать степень общественной опасности последствий от противоправного информационно-телекоммуникационного воздействия. Не всегда поддается определению и вероятность их наступления, в то время как кумулятивный эффект от негативной трансформации индивидуального и (или) общественного сознания может быть весьма опасным не только в ближайшем, но и отдаленном будущем. В отношении информационных воздействий подобного рода отметим, что повышается актуальность приведенного более полувека назад утверждения российского ученого В. Н. Кудрявцева о сравнительно большей степени опасности тех действий, которые

³⁵ Подробнее см.: Ключко Р. Н. Информационное действие как вид преступного поведения и особенности его уголовно-правовой оценки // Судовы Веснік. 2018. № 2 (106). С. 71—72.

³⁶ Утв. распоряжением Правительства РФ от 2 декабря 2015 г. № 2471-р.

обладают более высокой вероятностью наступления вредных последствий³⁷.

Именно предполагая тяжесть и вероятность наступления общественно опасных последствий для личности от размещения «фейковой» информации, «объектив» современного уголовного закона важно обратить на криминализацию использования цифровых технологий для целей распространения сведений ложного, порочащего и оскорбительного содержания. Для этого опытной площадкой могут стать нормы уголовных кодексов Азербайджана (ст. 147, 148), Беларуси (ст. 188, 189) и Казахстана (ч. 2 ст. 131) об ответственности за массовое распространение оскорбительных сведений через ресурсы сети Интернет. «Барометром» новейшей для многих государств — участников СНГ тенденции — стремительной криминализации публичного распространения заведомо ложных сведений, создающих опасность нарушения общественного порядка и наступления тяжких последствий, — явились практические потребности противодействия пандемии COVID-19. Например, 26 марта 2020 г.³⁸ УК Узбекистана был дополнен ст. 244-5 об ответственности за распространение не соответствующих действительности сведений о карантинных и других опасных для человека инфекциях. В части второй этой статьи квалифицирующим признаком признан публичный характер совершения таких деяний — в печатном или иным способом размноженном тексте, в средствах массовой информации либо в сети Интернет. Весной 2020 г. ответственность за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, появилась в ст. 207¹ УК РФ³⁹, хотя в некоторых государствах — участниках СНГ нормы такой направленности действуют уже продолжительный период времени. В частности, ст. 340 УК Беларуси определяет наказуемость заведомо ложных сообщений об опасности. В статье 274 УК Казахстана общественно опасным признается распространение заведомо ложной информации, в том числе через сети телекоммуникаций.

Как показал представленный компаративный обзор, нередко в уголовных кодексах тех или иных стран видовой состав правонарушений, в которых

сопряженность с «цифровым» признаком является криминообразующим обстоятельством, различен, и их число умножается в геометрической прогрессии, иногда опережая новациями модельное законодательство МПА СНГ. Увеличение в уголовных кодексах государств — участников СНГ количества новых правонарушений подобной направленности, как правило, в течение небольшого временного интервала, позволяет говорить о коэффициенте нестабильности уголовного закона⁴⁰. Однако наличие этого коэффициента вполне объяснимо не столько вызовами технологической революции, сколько угрозами общественного спокойствия, продуцируемыми современными реалиями. Еще Т. Джефферсон отмечал, что любой закон «по мере того, как он развивается, становится более просвещенным с новыми открытиями, установлением новых истин и изменением нравов и взглядов ввиду изменившихся условий» должен «улучшаться и идти в ногу со временем»⁴¹.

Современные темпы цифровизации экономики полицентричны, они сравнимы со скоростью вращения галактик, и с каждым годом этот процесс втягивает все больше государств-партнеров региональной евразийской интеграции. В национальных правовых системах соседствующих с нами стран активно апробируются технологии «блокчейн», переносятся из теневой экономики в правовое поле цифровые финансовые активы (криптовалюта, токены)⁴² и деятельность криптобирж, развиваются модели е-правосудия и народного финансирования интернет-платформ (краудфандинг), предпринимаются шаги к легитимации искусственного интеллекта. Например, в 2017 г. регуляторные механизмы внедрения в национальную экономику технологии «блокчейн» и оборота виртуальных активов легитимированы в Беларуси⁴³ и Казахстане⁴⁴. В 2018 г. в Узбекистане кроме этих институтов⁴⁵ в легальную область лицензирова-

⁴⁰ О понятии и формулах расчета «коэффициентов стабильности» и «нестабильности» уголовного закона см.: Анализ стабильности отдельных законодательных актов в сфере правоохранительной деятельности: науч. издание / под ред. Р. К. Сарпекова. Нур-Султан, 2019. С. 17—18.

⁴¹ Цит. по: Сытин А. Г. Политическая философия демократии: вклад Томаса Джефферсона // Полис. Политические исследования. 2008. № 1 (103). С. 162.

⁴² Подробнее см.: Кучеров И. И. Криптовалюта (идеи правовой идентификации альтернативных платежных средств): монография. М., 2018. С. 158—165.

⁴³ См., например, декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики».

⁴⁴ См., например, постановление Правительства Республики Казахстан от 12 декабря 2017 г. № 827 «Об утверждении Государственной программы “Цифровой Казахстан”».

⁴⁵ См., например, постановление Президента Республики Узбекистан от 3 июля 2018 г. № ПП-3832 «О мерах по развитию цифровой экономики в Республике Узбекистан»; Концеп-

³⁷ См.: Кудрявцев В. Н. Объективная сторона преступления. М., 1960. С. 65.

³⁸ См. Закон Республики Узбекистан от 26 марта 2020 г. № ЗРУ-613 «О внесении изменений и дополнений в Уголовный, Уголовно-процессуальный кодексы Республики Узбекистан и Кодекс Республики Узбекистан об административной ответственности».

³⁹ См. Федеральный закон от 1 апреля 2020 г. № 100-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации».

ния переведена деятельность криптобирж⁴⁶. Охватывая «кросс-отраслевые» процессы цифровая трансформация экстравертна и циклична⁴⁷. Она не только вскрывает необходимость устранения вакуума в легитимации новых цифровых продуктов в сфере частного права, но и внедряется в более консервативную «экосистему» публичного права. Одной из эффективных практик такого внедрения является адаптация «электронной проксемики»⁴⁸ уголовно-юрисдикционной деятельности в Казахстане⁴⁹.

Появление новых продуктов распределенных реестров прогнозирует тенденцию к установлению границ публично-правовой ответственности за злоупотребления при их капитализации, например непосредственно или в связи с легализацией активов, полученных преступным путем, финансированием терроризма и распространением оружия массового поражения (ПОД/ФТ). «Виртуальная реальность, складывающаяся в процессе цифровизации, — отмечает академик РАН Т. Я. Хабриева, — открывает не только новые горизонты социально-экономического развития общества, но и дополнительные, ранее не существовавшие возможности для совершения правонарушений, в частности, преступлений», предметом совершения которых все чаще становятся цифровые технологии оборота виртуальных активов⁵⁰.

цию совершенствования гражданского законодательства Республики Узбекистан: приложение № 1 к распоряжению Президента Республики Узбекистан от 5 апреля 2019 г. № Р-5464 «О мерах по совершенствованию гражданского законодательства Республики Узбекистан».

⁴⁶ См., например, постановление Президента Республики Узбекистан от 2 сентября 2018 г. № ПП-3926 «О мерах по организации деятельности криптобирж в Республике Узбекистан».

⁴⁷ Подробнее см.: Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 90—94. DOI: 10.12737/art_2018_1_7; Хабриева Т. Я. Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики: стратегические задачи и правовые решения // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 462. DOI: 10.17150/2500-4255.2018.12(4).459-467.

⁴⁸ См., например: Рябцева Е. В. Правовая модель информационного общества через призму доступности правосудия // Информационное право. 2016. № 3. С. 4—7.

⁴⁹ Подробнее см.: Голованова Н. А., Гравина А. А., Зайцев О. А. и др. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. М., 2019. С. 192—211; Зайцев О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 42—57. DOI: 10.12737/jflcl.2019.4.4.

⁵⁰ См.: Хабриева Т. Я. Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финан-

Учитывая транснациональный характер отмывания преступных доходов⁵¹ и признание проблематики разработки мер противодействия ей предметом не только национальных, но и международных научных исследований⁵², представляется, что попытки создать систему таких мер в рамках одного государства не будут обладать должным уровнем продуктивности. Эти шаги должны носить коллективный характер в русле «интеграции интеграций»⁵³, объединяя и гармонизируя усилия стран-партнеров на площадках различных региональных интеграционных объединений на евразийском пространстве. Межгосударственное сотрудничество на платформе государств — участников СНГ в области инновационных подходов к ПОД/ФТ иллюстрирует трансформацию региональных интеграционных процессов, характеризующуюся их смещением в направлении вновь образованных «колец» интеграции. Наблюдается расширение евразийской модели интеграции, пересечение сферы одного интеграционного объединения с платформами других межгосударственных организаций интеграционного типа. Это обусловлено тем, что в современный период каждое из государств — участников СНГ входит уже не в одно, а в два (и даже более) региональных соглашения. Иными словами, имеет место пролиферация, которая, приобретая так называемый эффект спагетти⁵⁴, существенно расширяет географию интеграционных процессов и приводит к их панъевразийности. Евразийская региональная интеграция идет по пути трансверсальности, предлагая унифицированные правовые регуляторы новых цифровых продуктов и в рамках платформы СНГ, и в плоскостях иных интеграционных объединений, прежде всего Евразийского экономического союза (ЕАЭС)⁵⁵.

Однако применительно к публичной сфере, особенно в части уголовно-правового регулирования, следует учитывать разновекторность этих двух ин-

сированию терроризма в условиях цифровизации экономики: стратегические задачи и правовые решения. С. 460.

⁵¹ См. Конвенцию ООН против транснациональной организованной преступности 2000 г. (ст. 6, 7).

⁵² См.: Хабриева Т. Я. Участие научного сообщества России в национальной антиотмывочной системе // Финансовая безопасность. 2019. № 24. С. 6—7, 11, 14—15.

⁵³ См.: Интеграционные процессы в Европе и Евразии: роль конвенций Совета Европы: сб. статей и выступлений. М., 2017. С. 7—8, 11—12, 60—75.

⁵⁴ См., например: Михалева Т. Н. Профессионально об актуальном: интеграционные модели современности: институциональные и юридические аспекты. URL: <http://pravo.by/novosti/novosti-pravo-by/2018/november/31312/>.

⁵⁵ См. также: Ковлер А. И., Белялова А. М., Лукьянова В. Ю. и др. Исследовательские центры международных организаций и их вклад в развитие правового регулирования региональной интеграции на евразийском пространстве: монография / под общ. ред. А. И. Ковлера. М., 2019. С. 132—133.

теграционных объединений. Конечно, весомый потенциал для евразийской интеграции имеет регуляторика Евразийской экономической комиссии (ЕЭК) ЕАЭС, в которой, в частности, заложены ориентиры регламентации электронных услуг. Вместе с тем регуляторная база ЕЭК ЕАЭС в большинстве случаев ориентирована на экономическую интеграцию, в то время как в нормативных правовых актах МПА СНГ дополнительно концентрируется внимание на гармонизации законодательства в вопросах противодействия современным вызовам и угрозам безопасности и правопорядка⁵⁶. Вероятно, этот нюанс объясняет отсутствие в потенциале ЕЭК ЕАЭС «эталонных» норм «жесткого права» (как это имеет место в правовой базе МПА СНГ). Подобная лакуна обуславливает популярность научных исследований механизмов международно-правового сотрудничества в сфере предотвращения использования общего финансового рынка ЕАЭС для целей отмывания денег и финансирования терроризма. В свою очередь, усиление научной составляющей в данной области активно содействует гармонизации применения на евразийском континенте антиотмывочных требований Группы разработки финансовых мер по борьбе с отмыванием денег (ФАТФ)⁵⁷ на операции с виртуальными валютами. Так, следуя 15-й рекомендации ФАТФ по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг виртуальных активов (VASP), национальные юрисдикции в оперативные сроки должны принять правовые и практические меры по предотвращению злоупотреблений виртуальными активами, гармонизировав общие правила ПОД/ФТ на виртуальные активы⁵⁸.

Во многом с учетом данной рекомендации ФАТФ в Российской Федерации виртуальные активы (крип-

товалюта) признаны предметом легализации (отмывания) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ), либо приобретенных лицом в результате совершения преступления (ст. 174¹ УК РФ). Так, 26 февраля 2019 г. п. 1 постановления Пленума Верховного Суда РФ от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», был дополнен абз. 3 соответствующего содержания. Не преследуя в рамках настоящего компаративного обзора цели освещения теоретических и практических аспектов квалификации легализации денежных средств, преобразованных из полученных вследствие преступной деятельности виртуальных активов, предположим, что признание криптовалюты предметом этого деяния станет лишь первым шагом к ее легитимной «адаптации» в качестве криминообразующего признака. Полагаем, что аналогичный прием детализации обобщающих рекомендаций высшей судебной инстанции позволит апробировать в уголовном законе и судебной практике научную позицию о легализации виртуальной валюты в качестве предмета хищения чужого имущества⁵⁹ и незаконного вывода капиталов из национальной юрисдикции⁶⁰, а также как основного средства платежа при нелегальном наркообороте⁶¹ и распространении порноматериалов⁶².

⁵⁹ См., например: Сидоренко Э. Л. Хищение криптовалюты: парадоксы квалификации // Гуманитарные, социально-экономические и общественные науки. 2018. № 6. С. 166—171.

⁶⁰ См., например: Кудратов М., Печегин Д. А. Перемещение активов и незаконный вывод капиталов: актуальные проблемы противодействия // Журнал российского права. 2020. № 1. С. 101—111. DOI: 10.12737/jrl.2020.007; Кунев Д. А., Волеводз А. Г. К вопросу о противодействии перемещению преступных активов в иностранные юрисдикции и их возврате в страны происхождения // Международное уголовное право и международная юстиция. 2019. № 3. С. 3—4.

⁶¹ См., например: Сидоренко Э. Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2 (51). С. 8—13; Чирков Д. К. Совершенствование законодательства в сфере незаконного оборота наркотиков в связи с появлением криптовалюты как анонимного средства платежа // Наркоконтроль. 2018. № 2 (51). С. 14—17; Халиуллина Л. Г. Криптовалюты в механизме незаконного оборота наркотических средств и психотропных веществ // Наркоконтроль. 2019. № 3 (56). С. 23—26; Дудко Т. А. Преступления в сфере блокчейн-технологий // I Минские криминологические чтения: матер. Междунар. науч.-практ. конф. (Минск, 20 декабря 2018 г.): в 2 ч. Минск, 2018. Ч. 1. С. 142—145.

⁶² См., например: Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Березкин Ю. М., Суходолов Я. А. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологи-

⁵⁶ Подробнее см.: Zulfugarzade T. E., Tsirina M. A., Semykina O. I. Improvement of Legal Groundwork for the Online Dispute Resolution System // 13th International and Practical Conference — Artificial Intelligence Anthropogenic Nature vs. Social Origin. Volgograd, 2020. P. 792—800. DOI: 10.1007/978-3-030-39319-9_87.

⁵⁷ См.: Хабриева Т. Я. Участие научного сообщества России в национальной антиотмывочной системе. С. 10.

⁵⁸ См.: FATF (2012—2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France. URL: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>; Внесение изменений в стандарты ФАТФ и заявление ФАТФ по виртуальным активам (29 октября 2019 г.). URL: <http://www.fedsfm.ru/preparation-fatf-fourth-round/news/3508>; Рекомендации ФАТФ (FATF) по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг в сфере виртуальных активов (VASP) (Interpretive Note to Recommendation 15 on New Technologies (INR. 15)): Отчет (Москва, 4 июля 2019 г.). URL: <https://alrf.msk.ru/files/03654e0d164907fc4b7d1eae061779767.pdf>.

Развитие цифрового информационного общества требует решения вопросов корреляции цифровой действительности и содержания принципов действия уголовного закона по кругу лиц, в пространстве и во времени, развития института соучастия в преступлении, причинения и сопричинения вреда по неосторожности. Несмотря на то что уголовное законодательство традиционно принято считать самым консервативным, находящимся в режиме «ожидания перемен»⁶³, поиск новых юридических конструкций, позволяющих обеспечить баланс и соблюдение интересов всех их субъектов, является актуальной задачей уже сегодняшнего дня. В подтверждение этого пути трансформации обратимся к известной правовой позиции Конституционного Суда РФ: «В случаях, когда предусматриваемые уголовным законом меры перестают соответствовать социальным реалиям, приводя к ослаблению защиты конституционно значимых ценностей или, напротив, к избыточному применению государственного принуждения, законодатель обязан привести уголовно-правовые предписания в соответствие с новыми социальными реалиями»⁶⁴.

ческий журнал. 2019. Т. 13. № 1. С. 85—93. DOI: 10.17150/2500-4255.2019.13(1).85-93; Халиуллина Л. Г. Указ. соч. С. 23—26; Сидоренко Э. Л. Наркотики и криптовалюта: мировые криминологические тренды. С. 8—13; Чирков Д. К. Указ. соч. С. 14—17.

⁶³ Подробнее см.: Жалинский А. Э. Уголовное право в ожидании перемен: теоретико-инструментальный анализ. 2-е изд. М., 2013.

⁶⁴ Постановление КС РФ от 20 апреля 2006 г. № 4-П «По делу о проверке конституционности части второй статьи 10 Уголовного кодекса Российской Федерации, части второй статьи 3 Федерального закона “О введении в действие Уголовно-

Если рассматривать уголовное право и уголовное законодательство как своеобразный «слепок» современного общества с типичными для него характеристиками цифровизации и глобализации⁶⁵, детерминация новых деяний, сопряженных с «цифровым» способом их совершения, представляет собой лишь вопрос времени. Механизм уголовно-правовой охраны общественных отношений, складывающихся при производстве, обмене и потреблении цифровых и информационно-телекоммуникационных данных, должен использоваться для противодействия общественно опасным деяниям, причиняющим или создающим угрозу причинения вреда поставленным под охрану уголовного закона объектам. Возможно, с этих позиций следует задать предиктор пересмотра классических подходов к пониманию парадигмы преступления как явления реальной, объективной действительности с учетом появления действительности цифровой (виртуальной) и возможных угроз использования информационно-телекоммуникационного воздействия для причинения вреда уже существующим и могущим появиться в перспективе объектам уголовно-правовой охраны.

го кодекса Российской Федерации”, Федерального закона “О внесении изменений и дополнений в Уголовный кодекс Российской Федерации” и ряда положений Уголовно-процессуального кодекса Российской Федерации, касающихся порядка приведения судебных решений в соответствие с новым уголовным законом, устраняющим или смягчающим ответственность за преступление...».

⁶⁵ Подробнее см.: Рахманова Е. Н. Уголовно-правовые и криминологические проблемы противодействия преступности // Российское правосудие. 2019. № 5. С. 109.

Библиографический список

Global Terrorism Index 2019: Measuring the Impact of Terrorism. Sydney, 2019. P. 8—9. URL: <http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf>.

Zulfugarzade T. E., Tsrina M. A., Semykina O. I. Improvement of Legal Groundwork for the Online Dispute Resolution System // 13th International and Practical Conference — Artificial Intelligence Anthropogenic nature vs. Social Origin. Volgograd, 2020. DOI: 10.1007/978-3-030-39319-9_87.

Анализ стабильности отдельных законодательных актов в сфере правоохранительной деятельности: научное издание / под ред. Р. К. Сарпекова. Нур-Султан, 2019.

Артемов В. Ю., Власов И. С., Голованова Н. А. и др. Новые направления развития уголовного законодательства в зарубежных государствах: сравнительно-правовое исследование: монография / отв. ред. Н. А. Голованова, С. П. Кубанцев. М., 2019.

Бачило И. Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства: сб. науч. работ / отв. ред. И. Л. Бачило. М., 2015.

Власов И. С., Голованова Н. А., Меньших А. А. Ответственность за компьютерные преступления по законодательству зарубежных государств // Журнал зарубежного законодательства и сравнительного правоведения. 2005. № 2.

Выводы организаторов Конференции по противодействию международному терроризму, организованной МПА СНГ (18 апреля 2019 г., г. Санкт-Петербург). URL: <https://iacis.ru/upload/medialibrary/4fd/vyvody-organizatorov-konferentsii.pdf>.

Голованова Н. А. Новые формы онлайн-преступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. DOI: 10.12737/jflcl.2019.3.4.

Голованова Н. А., Гравина А. А., Зайцев О. А. и др. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. М., 2019.

Голованова Н. А. Уголовное право Англии: учеб. пособие для бакалавриата и магистратуры. М., 2017.

Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // *Lex russica*. 2018. № 4. DOI: 10.17803/1729-5920.2018.137.4.108-120.

Дубко М. А. Неправомерное завладение компьютерной информацией как преступление против информационной безопасности: автореф. дис. ... канд. юрид. наук. Минск, 2018.

Дубко М. А. Совершенствование уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией (ст. 352 УК) // *Вестник Академии МВД Республики Беларусь*. 2018. № 1 (35).

Дубко М. А. Основание и причины криминализации неправомерного завладения компьютерной информацией // *Вестник Академии МВД Республики Беларусь*. 2017. № 1 (33).

Дудко Т. А. Преступления в сфере блокчейн-технологий // *I Минские криминалистические чтения: матер. Междунар. науч.-практ. конф. (Минск, 20 декабря 2018 г.): в 2 ч. Минск, 2018. Ч. 1.*

Жалинский А. Э. Уголовное право в ожидании перемен: теоретико-инструментальный анализ. 2-е изд. М., 2013.

Зайцев О. А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // *Журнал зарубежного законодательства и сравнительного правоведения*. 2019. № 4. DOI: 10.12737/jflcl.2019.4.4.

Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Березкин Ю. М., Суходолов Я. А. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // *Всероссийский криминологический журнал*. 2019. Т. 13. № 1. DOI: 10.17150/2500-4255.2019.13(1).85-93.

Интеграционные процессы в Европе и Евразии: роль конвенций Совета Европы: сб. статей и выступлений. М., 2017.

Кибальник А. Г. Квалификация мошенничества в новом постановлении Пленума Верховного Суда РФ // *Уголовное право*. 2018. № 1.

Ключко Р. Н. Информационное воздействие: потенциальные угрозы и проблемы уголовно-правовой оценки // *Оптимизация правовой основы противодействия преступности: к 25-летию Конституции Российской Федерации: сб. науч. трудов по итогам Всерос. науч.-практ. конф. с междунар. участием, г. Волгоград, 12—13 дек. 2018 г.: в 2 ч. Ч. 1 / под ред. Л. В. Лобановой, С. М. Мкртчян; редкол.: Л. В. Лобанова (отв. ред.) и др. Волгоград, 2018.*

Ключко Р. Н. Информационное действие как вид преступного поведения и особенности его уголовно-правовой оценки // *Судовы Веснік*. 2018. № 2 (106).

Ключко Р. Н. Общественно опасное информационное воздействие: виды и особенности уголовно-правовой оценки // *Безопасность и устойчивое развитие: теория и практика в условиях цифровой трансформации: матер. Междунар. науч.-практ. конф. Минск, 5—6 декабря 2019 г.: в 5 т. / редкол.: Г. Г. Краско (гл. ред.) и др. Минск, 2019. Т. 3.*

Ключко Р. Н. Проблемы уголовно-правового воздействия за действия информационного характера // *Проблемы эффективности осуществления правоохранительной функции в обеспечении социально-экономической стабильности в обществе: сб. матер. Междунар. науч.-практ. конф. Минск, 9—10 нояб. 2018 г. / под ред. В. В. Марчука, А. В. Солтановича. Минск, 2018.*

Ковлер А. И., Белялова А. М., Лукьянова В. Ю. и др. Исследовательские центры международных организаций и их вклад в развитие правового регулирования региональной интеграции на евразийском пространстве: монография / под общ. ред. А. И. Ковлера. М., 2019.

Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / отв. ред. В. М. Лебедев. М., 2017. Т. 3: Особенная часть. Раздел IX.

Кудратов М., Печегин Д. А. Перемещение активов и незаконный вывод капиталов: актуальные проблемы противодействия // *Журнал российского права*. 2020. № 1. DOI: 10.12737/jrl.2020.007.

Кудрявцев В. Н. Объективная сторона преступления. М., 1960.

Кунев Д. А., Волеводз А. Г. К вопросу о противодействии перемещению преступных активов в иностранные юрисдикции и их возврате в страны происхождения // *Международное уголовное право и международная юстиция*. 2019. № 3.

Кучеров И. И. Криптовалюта (идеи правовой идентификации альтернативных платежных средств): монография. М., 2018.

Макаров О. С., Баньковский А. Л. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь. URL: <https://zakonrb.com/npa/makarov-os-bankovskiy-al-konceptualnye-napravleniya>.

Михалева Т. Н. Профессионально об актуальном: интеграционные модели современности: институциональные и юридические аспекты. URL: <http://pravo.by/novosti/novosti-pravo-by/2018/november/31312/>.

Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // *Вестник УрФО. Безопасность в информационной сфере*. 2019. № 3 (33). DOI: 10.14529/secur190307.

Программа сотрудничества государств — участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2020—2022 годы (утв. Решением Совета глав государств СНГ от 11 октября 2019 г.).

Профилактика терроризма и экстремизма в молодежной среде. СПб., 2018.

Расулев А. Концептуальные основы уголовно-правовой охраны информационных отношений в Республике Узбекистан // *Правосудие (Одил судлов)*. 2019. № 1.

Рахманова Е. Н. Уголовно-правовые и криминологические проблемы противодействия преступности // *Российское правосудие*. 2019. № 5.

Рахмон Д. С. Некоторые вопросы, связанные с правовой защитой национальных интересов и национальной безопасности в условиях глобальных вызовов и угроз // Правовая жизнь. 2019. № 3 (27).

Русскевич Е. А. Отграничение кражи с банковского счета или в отношении электронных денежных средств от смежных составов преступлений // Уголовное право. 2019. № 2.

Рябцева Е. В. Правовая модель информационного общества через призму доступности правосудия // Информационное право. 2016. № 3.

Семыкина О. И. Актуализация ответственности за хищения с использованием кибертехнологий в свете экономических угроз: опыт регламентации в законодательстве зарубежных государств // Электронная валюта в свете современных правовых и экономических вызовов: сб. матер. междунар. науч.-практ. конф. (2 июня 2016 г.) / редкол.: А. С. Генкин, Э. Л. Сидоренко, О. И. Семыкина. М., 2016.

Семыкина О. И. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6 (61). DOI: 10.12737/23525.

Сидоренко Э. Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2 (51).

Сидоренко Э. Л. Хищение криптовалюты: парадоксы квалификации // Гуманитарные, социально-экономические и общественные науки. 2018. № 6.

Сухаренко А. Н. Антитеррористическое сотрудничество государств СНГ: состояние и тенденции // Диалог: политика, право, экономика. 2018. № 4 (11).

Сытин А. Г. Политическая философия демократии: вклад Томаса Джефферсона // Полис. Политические исследования. 2008. № 1 (103).

Уголовный кодекс Республики Беларусь: науч.-практ. коммент. / под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. Минск, 2019.

Хабриева Т. Я. Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в условиях цифровизации экономики: стратегические задачи и правовые решения // Всероссийский криминологический журнал. 2018. Т. 12. № 4. DOI: 10.17150/2500-4255.2018.12(4).459-467.

Хабриева Т. Я. Участие научного сообщества России в национальной антиотмывочной системе // Финансовая безопасность. 2019. № 24.

Хабриева Т. Я., Андриченко Л. В., Цирин А. М. и др. Организационно-правовые механизмы противодействия коррупции в субъектах Российской Федерации: монография. М., 2019. DOI 10.31085/9785392288113-2019-224.

Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. DOI: 10.12737/art_2018_1_7.

Халиуллина Л. Г. Криптовалюта в механизме незаконного оборота наркотических средств и психотропных веществ // Наркоконтроль. 2019. № 3 (56).

Чирков Д. К. Совершенствование законодательства в сфере незаконного оборота наркотиков в связи с появлением криптовалюты как анонимного средства платежа // Наркоконтроль. 2018. № 2 (51).

Шаухаров К. Уголовные правонарушения в сфере информатизации и связи // Заңгер — Вестник права Республики Казахстан. 2017. № 3 (188).

Шибяев Д. В. Методы противодействия информационной войне // Российский журнал правовых исследований. 2016. № 4 (9). DOI: <https://doi.org/10.17816/RJLS18192>.

Юсупов Р. М., Бачило И. Л., Бондуровский В. В., Вус М. А., Макаров О. С. Правовой вектор обеспечения информационной безопасности в модельном законодательстве СНГ // Диалог: политика, право, экономика. 2017. № 2 (5).

“Digital” Element of Crimes as Vector of Criminalization (Comparative Review of Approaches of CIS Member States)

O. I. Semykina^a, R. N. Klyuchko^b

^aInstitute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation

^bYanka Kupala State University of Grodno, Grodno 230023, Republic of Belarus

E-mail: semykola@yandex.ru; klrn.grodno@tut.by

DOI: 10.12737/jflcl.2020.051

Digital technologies that create tremendous opportunities to increase the speed and change forms of information interaction between various subjects of public relations (informatization), give rise to a change in their content. The search, receipt, transfer, collection, processing, accumulation, storage, distribution, provision, use and protection of information, the use of digital and other telecommunication technologies for these same actions have formed a “super-institute” of information relations that requires adequate measures of protection against unlawful influence and respect for confidentiality. The legal regulation of information relations should ensure their development, taking into account the needs of various entities (individuals, legal persons, society,

state, international community), and the criminal law protection should ensure the information security and information sovereignty of the relevant entities, preventing of violations of the legal status of relevant entities and opposition to the use of “digital” objects for criminal purposes.

Intensive digital transformation is changing the way we understand, first of all, information security. Today information security firstly is an integral element of informational relations. Secondly, it is associated with ensuring information sovereignty and thirdly it acts as an additional object of all crimes against the rights, freedoms and legitimate interests of individuals, society and the state, committed through digital exposure. This understanding of information security allows the authors to propose adjustments to the criminal law model for CIS Member-States and the criminal laws of some members of this integration association (for example, the Russian Federation and the Republic of Belarus) regarding the revision of approaches to determining the object of criminal law protection from cybercrimes “in pure form”.

The research is based on comparative, analytical and extrapolation methods. The article highlights the features of criminalization in the Model Criminal Code for the CIS member states and in the national criminal codes of the respective countries of two groups of criminal offenses — cyber offenses and informational offenses. The authors pay special attention to establishing responsibility for those acts, which include the designated groups of criminal offenses. They also have the necessary level of innovation and meet global challenges and threats from the justification of destructive ideology and disturbances in public order.

Keywords: criminal code, model law, cybercrime, informational crime, informational relations, informational security, informational sovereignty, destructive informational and telecommunication influence, “digital” sign of crime.

For citation: Semykina O. I., Klyuchko R. N. “Digital” Element of Crimes as Vector of Criminalization (Comparative Review of Approaches of CIS Member States). *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2020, no. 6, pp. 34—52. (In Russ.) DOI: 10.12737/jflcl.2020.051

References

- Analysis of the stability of certain legislative acts in the field of law enforcement: Scientific publication. Ed. by R. K. Sarpekov. Nur-Sultan, 2019. Pp. 17—18. (In Russ.)
- Artemov V. Yu., Vlasov I. S., Golovanova N. A. et al. New Directions of the Development of Criminal Legislation in Foreign Countries: comparative law research. Ed. by N. A. Golovanova, S. P. Kubantsev. Moscow, 2019. 424 p. (In Russ.)
- Bachilo I. L. About approaches to systematization and codification of information legislation. *Systematization and codification of information legislation*. Ed. by I. L. Bachilo. Moscow, 2015. 216 p. (In Russ.)
- Chirkov D. K. Legislation improvement in the area of illicit drug trafficking due to emergence of cryptocurrency as an anonymous payment means. *Narkokontrol'*, 2018, no. 2 (51), pp. 14—17. (In Russ.)
- Commentary on the Criminal Code of the Russian Federation. Ed. by V. M. Lebedev. Moscow, 2017. Vol. 3: The special part. Section IX. 298 p. (In Russ.)
- Dubko M. A. Improving the criminal legal regulation of responsibility for the misappropriation of computer information (Article 352 of the Criminal Code). *Vestnik Akademii MVD Respubliki Belarus'*, 2018, no. 1 (35), pp. 133—137. (In Russ.)
- Dubko M. A. The basis and reasons for the criminalization of misappropriation of computer information. *Vestnik Akademii MVD Respubliki Belarus'*, 2017, no. 1 (33), pp. 87—91. (In Russ.)
- Dubko M. A. The misappropriation of computer information as a crime against information security. Cand. diss. thesis. Minsk, 2018. 26 p. (In Russ.)
- Dudko T. A. Crimes in the field of blockchain technologies. *I Minsk Forensic Readings: Materials of the International Scientific and Practical Conference (Minsk, December 20, 2018)*. Minsk, 2018. Part 1. Pp. 142—145. (In Russ.)
- Global Terrorism Index 2019: Measuring the Impact of Terrorism. Sydney, 2019. Pp. 8—9. Available at: <http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf>.
- Golovanova N. A. New Types of Online Crimes Abroad. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2019, no. 3, pp. 42—57. (In Russ.) DOI: 10.12737/jflcl.2019.3.4
- Golovanova N. A. The criminal law of England. Moscow, 2017. 188 p. (In Russ.)
- Golovanova N. A., Gravina A. A., Zaytsev O. A. et al. Jurisdictional lawful activities within the criminal law sphere framework in the context of digitalization. Moscow, 2019. 212 p. (In Russ.)
- Greben'kov A. A. The concept of information crimes, a place in the criminal legislation of Russia and a place of signs of information in the structure of their composition. *Lex russica*, 2018, no. 4, pp. 108—120. (In Russ.) DOI: 10.17803/1729-5920.2018.137.4.108-120
- Integration processes in Europe and Eurasia: the role of Conventions of the Council of Europe: Collection of articles and speeches. Moscow, 2017. 323 p. (In Russ.)
- Ivantsov S. V., Sidorenko E. L., Spasennikov B. A., Berezkin Yu. M., Sukhodolov Ya. A. Cryptocurrency-related crimes: key criminological trends. *Russian Journal of Criminology*, 2019, vol. 13, no.1, pp. 85—93. (In Russ.) DOI: 10.17150/2500-4255.2019.13(1).85-93
- Khabrieva T. Y. Counteraction to the legalization (laundering) of proceeds from crime and the financing of terrorism in the context of the digitization of economy: strategic objectives and legal solutions. *Russian Journal of Criminology*, 2018, vol. 12, no. 4, pp. 459—467. (In Russ.) DOI: 10.17150/2500-4255.2018.12(4).459-467

- Khabrieva T. Y. The participation of the Russian scientific community in the national anti-laundering system. *Finansovaya bezopasnost'*, 2019, no. 24, pp. 6—15. (In Russ.)
- Khabrieva T. Y., Andrichenko L. V., Tsirin A. M. et al. Organizational and Legal Mechanisms for Combating Corruption in the Subjects of the Russian Federation. Moscow, 2019. 224 p. (In Russ.) DOI 10.31085/9785392288113-2019-224.
- Khabrieva T. Y., Chernogor N. N. The Law in the Conditions of Digital Reality. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 1, pp. 85—102. (In Russ.) DOI: 10.12737/art_2018_1_7
- Khaliullina L. G. Cryptocurrency in the mechanism of illicit trafficking of drugs and psychotropic substances. *Narkokontrol'*, 2019, no. 3 (56), pp. 23-26. (In Russ.)
- Kibalnik A. G. Qualification of fraud in the new resolution of the Plenum of the Supreme Court of the Russian Federation. *Ugolovnoe pravo*, 2018, no.1, pp. 61—67. (In Russ.)
- Klyuchko R. N. Information action as a type of criminal behavior and features of its criminal law assessment. *Sudovy Vesnik*, 2018, no. 2 (106), pp. 71—72. (In Russ.)
- Klyuchko R. N. Information impact: potential threats and problems of criminal legal assessment. *Optimization of the legal framework for combating crime: on the 25th Anniversary of the Constitution of the Russian Federation: Sat. scientific Proceedings of the All-Russian. scientific-practical conf. from the international participation, Volgograd, December 12—13, 2018*. Part 1. Ed. by L. V. Lobanova, S. M. Mkrtchyan. Volgograd, 2018. Pp. 93—98. (In Russ.)
- Klyuchko R. N. Problems of criminal law impact for actions of an informational nature. *Problems of the effectiveness of the enforcement function in ensuring socio-economic stability in society: Sat. materials Intern. scientific-practical conf., Minsk, November 9—10, 2018*. Ed. by V. V. Marchuk, A. V. Soltanovich. Minsk, 2018. Pp. 61—65. (In Russ.)
- Klyuchko R. N. Socially dangerous informational impact: types and features of a criminal law assessment. *Security and Sustainable Development: Theory and Practice in B39 Digital Transformation: Materials of the Intern. Scientific Pract. Conf., Minsk, December 5—6, 2019*. Ed. by G. G. Krasko et al. Minsk, 2019. Vol. 3. Pp. 59—62. (In Russ.)
- Kovler A. I., Belyalova A. M., Luk'yanova V. Yu. et al. Research Centers of International Organizations and Their Contribution to the Legal Framework of Regional Integration of the Eurasian Space. Ed. by A. I. Kovler. Moscow, 2019. 176 p. (In Russ.)
- Kucherov I. I. Cryptocurrency (ideas of legal identification of alternative means of payment). Moscow, 2018. 204 p. (In Russ.)
- Kudratov M., Pechegin D. A. Movement of Assets and Illegal Withdrawal of Funds: Current Issues of Counteraction. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2020, no. 1, pp. 101—111. (In Russ.) DOI: 10.12737/jrl.2020.007
- Kudryavtsev V. N. The objective side of the crime. Moscow, 1960. 244 p. (In Russ.)
- Kunev D. A., Volevodz A. G. On the issue of countering the transfer of criminal assets to foreign jurisdictions and their return to countries of origin. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiya*, 2019, no. 3, pp. 3—8. (In Russ.)
- Makarov O. S., Ban'kovsky A. L. Conceptual directions of legal regulation in the field of information security of the Republic of Belarus. Available at: <https://zakonrb.com/npa/makarov-os-bankovskiy-al-konceptualnye-napravleniya>. (In Russ.)
- Mikhaleva T. N. Professionally about the current: integration models of the present: institutional and legal aspects. Available at: <http://pravo.by/novosti/novosti-pravo-by/2018/november/31312/>. (In Russ.)
- Polyakova T. A., Minbaleev A. V., Boychenko I. S. Conceptual approaches to the legal regulation of information security in the context of digitalization and transformation of law. *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere*, 2019, no. 3 (33), pp. 64—68. (In Russ.) DOI: 10.14529/secur190307
- Prevention of terrorism and extremism among young people. St. Petersburg, 2018. 96 p. (In Russ.)
- Rahmon D. S. Some issues related to the legal protection of national interests and national security in the face of global challenges and threats. *Pravovaya zhizn'*, 2019, no. 3 (27), pp. 6—13. (In Russ.)
- Rakhmanova E. N. Criminal law and criminological problems of combating crime. *Rossiyskoe pravosudie*, 2019, no. 5, pp. 109—112. (In Russ.)
- Rasulev A. Conceptual foundations of the criminal law protection of information relations in the Republic of Uzbekistan. *Pravosudie (Odil sudlov)*, 2019, no. 1, pp. 94—101. (In Russ.)
- Russkevich E. A. Differentiation of theft from a bank account or in relation to electronic money from related offenses. *Ugolovnoe pravo*, 2019, no. 2, pp. 59—64. (In Russ.)
- Ryabtseva E. V. The legal model of the information-oriented society through the prism of the access to justice. *Informatsionnoe pravo*, 2016, no. 3, pp. 4—7. (In Russ.)
- Semykina O. I. Actualization of the responsibility for theft using cyber technologies in the light of economic threats: the experience of regulation in the legislation of foreign countries. *Electronic currency in the light of modern legal and economic challenges: Sat. materials of international scientific and practical. Conference (June 2, 2016)*. Ed. by A. S. Genkin, E. L. Sidorenko, O. I. Semykina. Moscow, 2016. Pp. 449—452. (In Russ.)
- Semykina O. I. Combating cybercrime in foreign countries. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2016, no. 6 (61), pp. 104—113. (In Russ.) DOI: 10.12737/23525
- Shaukharov K. Criminal offenses in the field of informatization and communication. *Vestnik prava Respubliki Kazakhstan*, 2017, no. 3 (188), pp. 43—48. (In Russ.)
- Shibaev D. V. Methods of countering the information war. *Rossiyskiy zhurnal pravovykh issledovaniy*, 2016, no. 4 (9), pp. 60—68. (In Russ.) DOI: <https://doi.org/10.17816/RJLS18192>

- Sidorenko E. L. Drugs and cryptocurrency: World trends in criminology. *Narkokontrol'*, 2018, no. 2 (51), pp. 8—13. (In Russ.)
- Sidorenko E. L. Theft of cryptocurrency: paradoxes of qualification. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennyye nauki*, 2018, no. 6, pp. 166—171. (In Russ.)
- Sukharensko A. N. Antiterrorist Cooperation of the CIS States: State and Trends. *Dialog: politika, pravo, ekonomika*, 2018, no. 4 (11), pp. 32—39. (In Russ.)
- Sytin A. G. The Political Philosophy of Democracy: A Contribution from Thomas Jefferson. *Polis. Politicheskie issledovaniya*, 2008, no. 1 (103), pp. 153—168. (In Russ.)
- The Criminal Code of the Republic of Belarus: scientific and practical. commentary. Ed. by V. M. Khomich, A. V. Barkov, V. V. Marchuk. Minsk, 2019. 1000 p. (In Russ.)
- Vlasov I. S., Golovanova N. A. Men'shikh A. A. Responsibility for computer crimes under the laws of foreign countries. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2005, no. 2, pp. 122—123. (In Russ.)
- Vyvody organizatorov Konferentsii po protivodeystviyu mezhdunarodnomu terrorizmu, organizovannoy MPA SNG (18 april 2019, St. Petersburg). Available at: <https://iacis.ru/upload/medialibrary/4fd/vyvody-organizatorov-konferentsii.pdf>
- Yusupov R. M., Bachilo I. L., Bondurovsky V. V., Vus M. A., Makarov O. S. Legal Vector of Information Security in the Model Legislation of the CIS. *Dialog: politika, pravo, ekonomika*, 2017, no. 2 (5), pp. 47—55. (In Russ.)
- Zaytsev O. A. Osobennosti ispol'zovaniya elektronnoy informatsii v kachestve dokazatel'stv po ugovnomu delu: sravnitel'no-pravovoy analiz zarubezhnogo zakonodatel'stva. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2019, no. 4. DOI: 10.12737/jflcl.2019.4.4.
- Zhalinsky A. E. Criminal law in anticipation of change: theoretical and instrumental analysis. 2nd ed. Moscow, 2013. 400 p. (In Russ.)
- Zulfugarzade T. E., Tsirina M. A., Semykina O. I. Improvement of Legal Groundwork for the Online Dispute Resolution System. *13th International and Practical Conference — Artificial Intelligence Anthropogenic nature vs. Social Origin*. Volgograd, 2020, pp. 792—800. DOI: 10.1007/978-3-030-39319-9_87