### **ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ ОТНОШЕНИЙ**

Е. Ю. Антонова,

доктор юридических наук, профессор, Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации

# ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. В последние годы отмечается активное внедрение различных цифровых технологий в процесс совершения преступлений террористической направленности. Автор поставил перед собой цель выработать рекомендации по противодействию таким преступлениям. Для достижения этой цели были проанализированы различные формы преступной деятельности террористических формирований, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий. Определено, что развитие цифрового пространства и цифровых технологий способствует интенсивности терроризма, а также привело к изменению механизма совершения преступлений террористической направленности. Сделан вывод о том, что для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом пространстве и (или) с использованием цифровых технологий необходимы четкая стратегия и соответствующая нормативная правовая база.

**Ключевые слова**: цифровые технологии, цифровое пространство, преступления террористической направленности, идеология насилия, пропаганда терроризма, вербовка, финансирование, криминализация, противодействие

## THE USE OF DIGITAL TECHNOLOGIES IN THE COMMISSION OF TERRORIST CRIMES: PROBLEMS OF COUNTERACTION

**Abstract.** In recent years, there has been an active introduction of various digital technologies in the process of committing crimes of a terrorist nature. The author set himself the goal of developing recommendations for countering such crimes. To achieve this goal, various forms of criminal activity of terrorist groups committed in the digital space and (or) using digital technologies were analyzed. It is determined that the development of digital space and digital technologies contributes to the intensity of terrorism and led to a change in the mechanism for committing crimes of a terrorist nature. It is concluded that to ensure the effectiveness of measures to counter terrorist crimes committed in the digital space and (or) using digital technologies, a clear strategy and an appropriate regulatory legal framework are needed.

**Keywords:** Digital technologies, Digital space, Terrorist crimes, Ideology of violence, Propaganda of terrorism, Recruitment, Financing, Criminalization, Counteraction

Преступления в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий/систем/программ представляют естественную эволюцию преступности, обусловленную научно-техническим прогрессом и новыми разработками, и относятся к числу серьезных проблем современного мира.

Не являются исключением и преступления террористической направленности. Отмечается, что уровень терроризма продолжает расти, как и «технологические достижения, способствующие привлечению внимания и эмоционального воздействия террористов» [16. Р. 251]. Исследователями фиксируется прямая связь между цифровым (кибер-) пространством и различными формами социально-политической дестабилизации: антиправительственными демонстрациями, беспорядками и террористическим актами [14. Р. 1–34].

Заместитель секретаря Совета безопасности России Ю. Коков справедливо замечает, что наступает эра цифрового терроризма, который по масштабам возможных последствий может быть сопоставим с оружием массового уничтожения. По его данным в Интернете действует около 30 тыс. террористических и экстремистских сайтов [9]. Данные обстоятельства требуют серьезной работы по противодействию преступлениям террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

Формы преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Лица, вовлеченные в террористическую деятельность, активно используют современные цифровые технологии не только в процессе совершения преступлений, но и в повседневной жизни. Такие технологии применяются внутри террористических сообществ/организаций (далее – формирований) в качестве инструмента коммуникации, в том числе в процессе организации террористической деятельности, а также при вербовке членов террористических формирований, распространении идеологии насилия, пропаганды террористической деятельности, призывов к совершению конкретных террористических актов. Террористы стремятся донести такие сообщения, а также продемонстрировать свои противоправные деяния максимально широкой аудитории, поскольку основной их целью является дестабилизация общества, его моральная и политическая нестабильность.

При этом, распространяя через цифровое (кибер-) пространство информацию, не всегда соответствующую действительности (это может быть и дезинформация, слухи, угрозы применения насилия или изображения актов насилия), террористические формирования оказывают воздействие не только на возможных или действительных сторонников террористических воззрений, идеологии насилия (что используется в первую очередь для вербовки новых членов, радикализации, подстрекательства к терроризму, подрыва веры в социальные ценности), но и на прямых или косвенных жертв террористических актов (устрашение населения путем психологического манипулирования, распространения чувств повышенного беспокойства, тревоги, страха или паники среди населения) или на органы власти и международное сообщество в целом (дестабилизация деятельности органов власти или международных организаций либо воздействия на принятие ими решений).

Именно поэтому террористы стремятся адаптировать экстремальные средства коммуникации для привлечения внимания и видимости в глобальной медиасреде. Насилие террористов, в высшей степени опосредованное и зрелищное, порождает превращение атак в медиа-события, которые разворачиваются в гибридной медиасреде и укореняются в доступных возможностях и технологиях [17. Р. 1–17].

Для совершения пропагандистских действий террористические формирования задействуют широкий спектр технических средств: веб-сайты, чат-группы и чат-форумы, онлайн-журналы, платформы таких социальных сетей, как Twitter (заблокирован в РФ) и Facebook (экстремистская организация, запрещена в РФ), популярные видео- и файлообменные веб-сайты, например, YouTube. Поисковые системы Интернета упрощают нахождение террористического контента.

На слушаниях в подкомитете по информации и борьбе с терроризмом Комитета Национальной безопасности палаты представителей Правительства США были приведены примеры использования террористами систем искусственного интеллекта (далее – ИИ). Так, один из сторонников превосходства белой расы открыл огонь по двум мечетям в Крайстчерче (Новая Зеландия), убив 51 человека и ранив еще 49. Террорист смог транслировать нападение в прямом эфире на Facebook, потому что ИИ Facebook не счел отснятый материал достаточно ужасным. Затем видео было 300 000 раз успешно загружено на Facebook другими пользователями. Это доказывает, что технологии ИИ, призванные блокировать такие видео, еще не справляются с поставленной задачей. Более того, имеются факты, свидетельствующие о том, что ИИ Facebook снимает видео и продвигает террористический контент, который он должен был удалить [12].

Кроме того, через цифровое (кибер-) пространство происходит вербовка новых членов террористических формирований, их онлайн-обучение; планирование террористических атак.

Отмечается, например, что специализированные террористические сайты работают как онлайн-библиотеки идеологических текстов, платформы для вербовщиков и форумы для обмена информацией. Кроме того, фото- и видеоматериалы, игры (имитирующие террористические атаки и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста), учебные пособия и технические инструкции, подготовленные террористическими группами, способствуют радикализации их сторонников [14. Р. 1–34]. Пропагандистские материалы могут содержать идеологические или практические руководства, разъяснения, оправдания или рекламу деятельности террористов.

Так, в ходе проверки Шахунской городской прокуратурой Нижегородской области интернет-ресурсов, осуществляемой с использованием программы браузера: «Google Chrome», в поисковом ресурсе «Яндекс», при введении ключевых слов «Expedient Homemade Firearms», отобразился список интернет-сайтов, содержащий ссылки: <данные изъяты>. На указанных интернет-страницах размещены материалы с подробной информацией о способах самостоятельного изготовления оружия, проходит обсуждение этой информации. Доступ к информации свободный для всех пользователей, сайт и интернет-страницы не содержат ограничений к его доступу по кругу лиц, не требуется предварительной регистрации и пароля, ознакомиться

с содержанием данной интернет-страницы и скопировать материалы в электронном варианте может любой интернет-пользователь, ограничения на передачу, копирование и распространение отсутствуют [2].

Как отмечают специалисты, воздействие на компьютерную информацию позволяет преступнику «манипулировать эмоциями и сознанием потерпевшего, вызывая серьезные психофизиологические последствия. Психоэмоциональный эффект сравним по силе с эффектом от событий в реальном мире, в то же время он смоделирован путем изменения компьютерной информации» [6. С. 235]. К таким психологическим приемам и прибегают террористические формирования в процессе вербовки новых членов и пропаганды своей идеологии.

В науке отмечаются феноменальные успехи систем ИИ не только в области цифровых платформ, но и в материальной, непосредственной среде. Это видно на примере внедрения цифровых технологий (современной робототехники) в систему беспилотного управления транспортных средств, что облегчает совершение террористических актов. На практике уже встречаются случаи применения цифровых технологий, в том числе беспилотников, в процессе приготовительной и непосредственной террористической деятельности, в частности для доставки наркотиков, психоактивных веществ и других запрещенных предметов – оружия, взрывчатых веществ, взрывных устройств и пр.

Так, террористические группы все чаще используют беспилотники для наблюдения, взрывов и других действий. Сообщается, что ИГИЛ (запрещенная в РФ организация) начал использовать боевые дроны в Ираке и объявил о создании подразделения «Беспилотные летательные аппараты моджахедов» [15]. Кроме того, ИГИЛ провел несколько бомбардировок с использованием беспилотников, нацеленных как на гражданские, так и на военные цели, и даже предпринимал попытки атаковать беспилотниками глав государств [13]. По мере увеличения производства этих гаджетов и снижения себестоимости эти новшества станут более привлекательными и востребованными для отдельных террористов и групп. Ножи и грузовики все еще могут быть более простыми и дешевыми вариантами, но новые методы атаки также начнут реализовываться [15].

3D-принтеры также могут сделать сложные и дорогие технологии доступными для террористов. Так, напавший на немецкую синагогу в Йом-Кипур в начале октября 2019 г. использовал напечатанные на 3D-принтере компоненты самодельного оружия [15]. В 2020 г. немецкий террорист потратил всего 50 долларов на 3D-печать деталей для оружия, которое использовалось при попытке нападения в Галле [13].

Цифровое (кибер-) пространство используется и в качестве средства для совершения кибератак, призванных нарушить нормальное функционирование компьютерных систем, серверов с помощью компьютерных вирусов, вредоносных и шпионских программ или других средств неправомерного доступа к компьютерной информации. Для этих действий характерны такие черты террористического акта, как стремление путем устрашения населения способствовать дестабилизации деятельности органов власти или международных организаций, воздействовать на принятие ими решений и таким образом достичь политических или иных социальных целей.

Для достижения поставленных целей и эффективной деятельности террористические формирования привлекают значительные материальные ресурсы. Цифровое (кибер-) пространство и новые технологии только способствуют быстрому получению доходов, которые в последующем используются для нужд террористов. Как отмечает руководитель Антитеррористического центра СНГ А. Новиков, «произошла цифровая трансформация механизмов и каналов финансирования терроризма». В качестве источников доходов террористы используют онлайн-казино, прибегают к хищениям денег через подставные интернет-магазины и сайты-двойники, используют фишинговые и фарминг-атаки, несанкционированный доступ к банковским ресурсам и криптовалютным биржам [10]. Кроме того, через цифровое (кибер-) пространство террористические формирования обращаются с прямыми просьбами о пожертвованиях. Для этого используются веб-сайты, чат-группы, массовые рассылки сообщений с просьбами о пожертвованиях.

Так, Северо-Кавказский окружной военный суд вынес обвинительный приговор в отношении Ш., который опубликовал в Интернете призыв к сбору денежных средств на нужды ИГИЛ. Полученные деньги он перевел на счет террористической группировки [3]. В другом случае следствием и судом установлено, что М. перечислил через платежный терминал 7000 руб. на счет электронного кошелька, который использовался для сбора денежных средств с целью финансовой помощи членам группировки «Хайят Тахрир аш-Шам», являющейся структурным подразделением запрещенной террористической организации «Джебхат ан-Нусра» [5].

Веб-сайты используются и в качестве интернет-магазинов, предлагающих книги, аудио-, видеозаписи и иные материалы с соответствующим содержанием.

Преимущества использования цифрового пространства и (или) цифровых технологий обусловлены, во-первых, скоростью передачи данных и распространения информации (дезинформации), а также обработки большого массива информации, позволяющей, например, оперативно отыскивать сторонников, вербовать новых членов террористических формирований и т. д.; во-вторых, охватом неопределенно широкой аудитории и расширением географии распространения деструктивной идеологии насилия в условиях относительной анонимности; в-третьих, сложностью контролирования содержательной части распространяемой информации; в-четвертых, упрощением координации действий членов террористических формирований.

Кроме того, к очевидным преимуществам цифровых технологий относят возможность их использования на любых, в том числе представляющих опасность территориях (зоны военных конфликтов); физическую безопасность субъектов, их применяющих (при использовании опасных предметов – химических, отравляющих или взрывчатых веществ и др.) и сложность их обнаружения [1. С. 35].

Перечисленные и иные факторы во многих случаях увеличивают и степень общественной опасности совершаемых деяний, что должно быть отражено и в нормах уголовного закона.

Особо привлекательной для террористических формирований в этом плане является несовершеннолетняя аудитория, поскольку она не имеет необходимого жизненного опыта, устойчивых положительных ориентаций и является активным пользователем цифрового (кибер-) пространства. К тому же, как отмечается в на-

учной литературе, «подростки подвержены формированию установок на агрессивное поведение». Наиболее действенными в отношении них являются технологии разжигания агрессии посредством экстремистских лозунгов, политизации социально-экономических проблем, романтизации образов «отрицательных героев», навязывания идей, пропагандирующих насилие как социальную норму и погружения их в деструктивные интернет-сообщества [11. С. 127–130]. Для вербовки несовершеннолетних применяются популярные музыкальные видеоролики, компьютерные игры, мультипликационные фильмы, рассказы, поощряющие и прославляющие действия террористов, миссии террористов-смертников и др.

Так, трое 15-летних подростков с октября 2019 г. по июнь 2020 г. «путем общения в одной из социальных сетей и мессенджерах, придерживаясь идей анархизма... объединились в группу для последующего совместного осуществления террористической деятельности на территории города Канска». Распределив между собой роли, подростки самостоятельно проходили обучение путем чтения запрещенной, признанной решением суда экстремистской литературы и просмотра видеофильмов по изготовлению взрывчатых веществ и взрывных устройств в целях осуществления террористической деятельности. Они самостоятельно изготавливали взрывчатые вещества и взрывные устройства и отрабатывали их применение на практике в заброшенном доме, на пустырях и стройках с целью подготовки к совершению террористического акта путем подрыва здания полиции или УФСБ. В материалах дела фигурировали скриншоты переписок в социальных сетях, в которых фигуранты дела обсуждали, где и как приобрести компоненты взрывчатки. Кроме того, школьники намеревались «для наглядности» построить в игре Minecraft здание ФСБ и взорвать его [8].

Все вышесказанное подтверждается и специалистами в области противодействия терроризму. Так, директор Контртеррористического управления ООН В. Воронков отмечает, что террористы активно пользуются различными технологическими достижениями. Используя социальные сети, зашифрованные сообщения («даркнет»), они распространяют свою человеконенавистническую идеологию, собирают и переводят средства, радикализируют молодежь и вербуют новых сторонников, координируют теракты. Причем они задействуют алгоритмы социальных сетей так, чтобы как можно быстрее и шире распространять свой контент. Есть данные о попытках террористического подполья использовать лекарственные препараты для создания биологического оружия. Для доставки химических, биологических или радиологических материалов, террористы могут применять беспилотники, в том числе автоматические [4].

Для противодействия преступлениям террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий требуется выработка эффективных механизмов уголовно-правового воздействия, которые позволят своевременно реагировать на террористические угрозы в цифровой среде. Новые задачи стоят и перед правоохранительными органами, которые должны оперативно выявлять источник угрозы и блокировать его.

Несмотря на то, что в российское уголовное законодательство вносятся изменения: нормы дополняются квалифицирующим (особо квалифицирующим)

признаком «совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», видоизменяются и появляются новые нормы о преступлениях против компьютерной информации, пока нельзя констатировать наличие должной, эффективной системы мер уголовно-правового воздействия на лиц, совершающих рассматриваемые деяния в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Анализ норм уголовного закона показывает, что к настоящему времени законодатель усилил лишь ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 2052 УК РФ), в случае их совершения в цифровом (кибер-) пространстве (ч. 2). Во всех остальных нормах о преступлениях террористической направленности соответствующий квалифицирующий (особо квалифицирующий) признак отсутствует. Вместе с тем практика показывает, что цифровое (кибер-) пространство используется не только для распространения пропагандистской информации в террористических целях, но и для содействия террористической деятельности, включая вербовку новых членов террористических формирований, финансирование, обучение исполнителей, подстрекательство к совершению террористических актов и др.

Проведенный анализ различных форм преступной деятельности террористических формирований, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, позволяет констатировать:

- 1) развитие цифрового (кибер-) пространства (социальных сетей, электронных СМИ и других интернет-ресурсов), увеличение числа пользователей таким пространством и цифровыми технологиями/системами/программами способствует расширению идеологии насилия за счет активной пропагандистской деятельности террористических формирований, и как результат интенсивности терроризма;
- 2) использование цифровых технологий террористическими формированиями, по сути, ведет к изменению механизма совершения преступлений террористической направленности от стадии приготовления до оконченного преступления и сокрытия его следов.

Данные обстоятельства должны быть учтены и при выработке конструктивных, эффективных мер по противодействию преступлениям террористической направленности. Современные цифровые технологии необходимо активнее использовать в процессе выявления, раскрытия и расследования преступлений террористической направленности, особенно когда таковые совершаются в цифровом (кибер-) пространстве, а также с использованием ІТ-технологий. Важным аспектом в этой связи является возможность использования ИИ оперативно-разыскными подразделениями (например, система распознавания лиц, идентификация личности, номеров транспортных средств, мониторинг социальных сетей и т. д.).

Цифровое (кибер-) пространство может эффективно быть использовано для проведения оперативно-разведывательных действий, сбора информации, извлекаемой из сообщений на веб-сайтах, в чатах и других цифровых ресурсах, что будет способствовать своевременному предотвращению и пресечению террористических актов, сбору доказательственной базы для привлечения лиц к уголовной ответственности.

Еще одной контрмерой является создание веб-сайтов, чат-групп, чат-форумов и других интернет-платформ для ведения конструктивных онлайн-дискуссий, демонстрации контртеррористических и иных воспитательно-просветительских материалов, опирающихся на конкретные факты, изложения альтернативных насильственным методов решения политических и иных социальных проблем.

Для эффективного выявления, раскрытия и расследования преступлений террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, сотрудники правоохранительных органов должны обладать не только правовыми, но и специальными техническими знаниями по механизму данных преступлений. Они должны знать современные цифровые (компьютерные, информационно-коммуникационные) технологии/системы/программы, порядок их работы.

Таким образом, для обеспечения эффективности мер по противодействию преступлениям террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий, необходима четкая стратегия и соответствующая нормативная правовая база, которые должны быть нацелены на:

- 1) криминализацию (изменение интенсивности пенализации) общественно опасных деяний (в том числе террористической направленности), совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий. Для этого необходима ревизия уголовного закона и иных нормативных правовых актов в сфере цифровых технологий в целях выявления пробелов правовой защиты объектов от террористических угроз и определения потребности усиления ответственности в конкретных случаях. Допускаем, что совершение преступлений в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий не во всех случаях может увеличивать степень общественной опасности запрещенных деяний. В этой связи на современном этапе считаем достаточным дополнить ст. 63 УК частью 12 и изложить ее в следующей редакции «12. Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать отягчающим обстоятельством совершение преступления с использованием цифровых и информационно-телекоммуникационных технологий»;
- 2) усиление сил и средств на воспитательно-просветительскую деятельность, в том числе в цифровом (кибер-) пространстве, направленную на пропаганду «мирного сосуществования всех народов независимо от расы, национальности, языка, происхождения в противовес негативному информационно-идеологическому воздействию на личность извне, в том числе пропаганды идеологии терроризма» [7. С. 207];
- 3) обучение сотрудников правоохранительных органов, выявляющих и расследующих преступления, в том числе террористической направленности, совершаемых в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий;
- 4) расширение полномочий сотрудников правоохранительных органов для обеспечения четкого и эффективного контроля цифрового контента;
- 5) выработку соглашений по международному сотрудничеству в области противодействия преступлениям, в том числе террористической направленности, совершаемым в цифровом (кибер-) пространстве и (или) с использованием цифровых технологий.

#### Список литературы

- 1. Антонова Е. Ю. Технологии искусственного интеллекта субъект преступления или орудие/средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 1 (14). С. 31–39. DOI: https://doi.org/10.31429/20785836–14–1–31–39
- 2. Архив Шахунского районного суда Нижегородской области. Решение № 2A-214/2021 от 22 марта 2021 г. Дело № 2A-214/2021 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/AAQ1OEJsQbb9/ (дата обращения: 27.07.2022).
- 3. В Дагестане суд приговорил собиравшего средства для ИГ мужчину к 17 годам // PБК. URL: https://www.rbc.ru/rbcfreenews/5d44544c9a7947190c12566e (дата обращения: 26.07.2022).
- 4. В Минске обсуждают возможности новых технологий и искусственного интеллекта в борьбе с терроризмом // Организация Объединенных Наций. URL: https://news.un.org/ru/story/2019/09/1362292 (дата обращения: 30.07.2021).
- 5. В Российской Федерации вынесен приговор за финансирование терроризма // Eurasian Group. URL: https://eurasiangroup.org/ru/sentence-for-terrorist-financing-in-russian-federation34 (дата обращения: 26.07.2022).
- 6. Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. Москва: Юрлитинформ. 328 с.
- 7. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. Москва: Академия управления МВД России, 2021. 244 с.
- 8. Подростка из Канска приговорили к 5 годам колонии за подготовку теракта // Деловой Петербург. URL: https://www.dp.ru/a/2022/02/10/Podrostka\_iz\_Kanska\_prigo (дата обращения: 27.07.2022).
- 9. СБ РФ: цифровой терроризм может быть сопоставим с оружием массового уничтожения // TACC. URL: https://tass.ru/politika/14658343/amp (дата обращения: 27.07.2022).
- 10. Террористы все активнее используют IT-технологии, заявили в АТЦ СНГ // РИА Новости. URL: https://ria.ru/amp/20200218/1564913906.html (дата обращения: 26.07.2022).
- 11. Щетинина Е. В. Проблемы развития культуры насилия в интернет-пространстве // Инновационное развитие профессионального образования. 2018. № 2 (18). С. 127–130.
- 12. Artificial Intelligence and Counterterrorism: Possibilities and Limitations // Hearing Before the Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives One Hundred Sixteenth Congress. First Session. June 25, 2019. Serial № 116–28. Washington: U. S. Government Publishing Office, 2020. 48 p.
- 13. Gavin J. Trends in Terrorism [2022] // Vision of Humanity. URL: https://www.visionofhumanity.org/trends-in-terrorism/ (дата обращения: 26.07.2022).
- 14. Khokhlov N., Korotayev A. Internet, Political Regime and Terrorism: A Quantitative Analysis // Cross-Cultural Research. 2022. Vol. 0 (0). Pp. 1–34. DOI: 10.1177/10693971221085343

- 15. Noor E. Sharing space: Tech and terrorism // Observer Research Foundation. URL: https://www.orfonline.org/expert-speak/sharing-space-tech-terrorism-60862/ (дата обращения: 25.07.2022).
- 16. Orehek E., Vazeou-Nieuwenhuis A. Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism // Policy Insights from the Behavioral and Brain Sciences. 2014. Vol. 1 (1). Pp. 248–255.
- 17. Uusitalo N., Valaskivi K., Sumiala J. Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence // Journalism. 2021. 16 May. Pp. 1–17. DOI: 10.1177/14648849211015601

#### Т. П. Афонченко,

кандидат юридических наук, доцент, Белорусский торгово-экономический университет потребительской кооперации

#### К ПРОБЛЕМЕ СОВЕРШЕНСТВОВАНИЯ УГОЛОВНО-ПРАВОВЫХ НОРМ В КОНТЕКСТЕ ВЫЗОВОВ ИНФОРМАТИЗАЦИИ

Аннотация. Целью представленного исследования является анализ проблем криминализации отдельных видов составов преступлений (хищений), совершаемых посредством использования цифровых технологий, в том числе в глобальной сети Интернет, в контексте обеспечения прав на безопасность каждого индивида. На основе изучения действующих нормативных актов формулируются предложения по совершенствованию национального уголовного законодательства Республики Беларусь посредством усиления уголовно-правовой репрессии в отношении виновных, использующих цифровую среду и цифровые технологии в качестве места и способа совершения преступления.

**Ключевые слова**: цифровые технологии, информационно-коммуникативная среда, преступное посягательство, уголовно-правовое воздействие, объект уголовно-правовой охраны, способ совершения преступления, мошенничество

### TO THE PROBLEM OF IMPROVEMENT OF CRIMINAL LEGAL NORMS IN THE CONTEXT OF INFORMATIZATION CHALLENGES

**Abstract.** The purpose of the presented study is to analyze the problems of criminalization of certain types of offenses (theft) committed through the use of digital technologies, including on the global Internet, in the context of ensuring the rights to security of each individual. Based on the study of the current regulations, proposals are formulated to improve the national criminal legislation of the Republic of Belarus by strengthening criminal law repression against the perpetrators who use the digital environment and digital technologies as a place and method of committing a crime.

**Keywords:** Digital technologies, Information and communication environment, Criminal infringement, Criminal legal impact, Object of criminal legal protection, Method of committing a crime, Fraud