Список литературы

1. Демидова-Петрова Е. В. Современные молодежные субкультуры криминальной и экстремистской направленности: особенности, виды // Мониторинг правоприменения. 2022. № 2 (43). С. 62–69.

2. Молодежь 2030. URL: https://www.un.org/youthenvoy/wp-content/uploads/2014/09/WEBR-UN-Youth-Strategy_Booklet_-Russian-for-WEB.pdf (дата обращения: 21.06.2022).

3. Гаврилов Б. Я. Суицид несовершеннолетних как форма отклоняющегося поведения в условиях современного общества: меры уголовно-правовой ответственности // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 4 (46). С. 463–471.

4. Солдатова Г. В., Зотова Е. Ю. Зона риска. Российские и европейские школьники: проблема онлайн-социализации // Дети в информационном обществе. 2011. № 7. С. 46–55.

5. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. Москва: Фонд Развития Интернет, 2013. 144 с.

6. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн. URL: https://www.thinkwithgoogle.com/intl/ru-ru/insights-trends/user-insights/novoe-pokolenie-internet-polzovatelei-issledovanie-privychek-i-povedeniia-rossiiskoi-molodezhi-onlain/ (дата обращения: 01.06.2022).

Д. Е. Дроздов,
кандидат юридических наук,
Калужский государственный
университет имени К. Э. Циолковского

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Аннотация. Исследована специфика современной преступности в цифровой среде и ее качества анонимности и латентности. Определены основные угрозы связанные с распространением идеологии экстремизма и терроризма, незаконным оборотом запрещенных предметов и веществ, легализацией доходов, полученных преступным путем. Предложены и обоснованы механизмы международного сотрудничества, связанные с обменом актуальной информацией и передовыми формами противодействия преступности.

Ключевые слова: цифровая преступность, цифровая среда, предупреждение преступности; профилактическая программа; терроризм, экстремизм, международное сотрудничество

THE MAIN DIRECTIONS OF DIGITAL CRIME PREVENTION

Abstract. The specifics of modern crime in the digital environment and its qualities of anonymity and latency are investigated. The main threats associated with the spread

of the ideology of extremism and terrorism, illegal trafficking of prohibited items and substances, legalization of proceeds from crime have been identified. Mechanisms of international cooperation related to the exchange of up-to-date information and advanced forms of crime prevention are proposed and substantiated.

Keywords: Digital crime, Digital environment, Crime prevention; Prevention program; Terrorism, extremism, International cooperation

Развитие наук уголовно-правового цикла обусловлено потребностями общества. Современная криминология находится в процессе накопления и систематизации знаний, что подразумевает не только уточнение предмета исследования и составных элементов, но и появление новых частных криминологических теорий. Подавляющее большинство сфер общественной полезной деятельности переходят в цифровую среду, что повышает вероятность возникновения угроз безопасности. В частности, вслед за ней, а зачастую опережая в цифровую среду проникает преступность, приобретая характер организованности, транснациональности и профессиональности, что значительно повышает ее опасность и увеличивает негативные последствия. Приобретая анонимность, обезличенность за счет специфики функционирования среды облегчается процесс совершения конкретного преступления и минимизируются издержки, в частности расширяются возможности и объемы распространения наркотических средств и психотропных веществ, финансирования террористический и экстремистской деятельности, легализации доходов полученных в результате совершения преступлений и т. д. Анонимность, отсутствие материальных следов преступной деятельности, трудности выявления и документирования особенно в случаях придания ей внешних признаков легальной деятельности стали причинами высокого уровня латентности.

Под преступностью традиционно понимается исторически изменчивое, неизбежное социально-правовое, относительно массовое явление, включающее совокупность запрещенных уголовным законом общественно опасных деяний, совершаемых в течение определенного периода времени на определенной территории [4. С. 57]. Качество исторической изменчивости наряду с научно-техническим прогрессом предопределили появление преступности в цифровой сфере, которая продолжает трансформироваться параллельно с совершенствованием информационных технологий.

Угрозы в цифровой сфере многообразны. Среди основных выделяются:

– Распространение идеологии терроризма и экстремизма, включая многообразие форм пропаганды не только с использованием социальных сетей и мессенджеров, но и онлайн-игр, позволяющих общаться в режиме реального времени.

– Незаконный оборот наркотических средств, психотропных веществ.

– Незаконный оборот оружия.

– Незаконный оборот материалов порнографического характера.

– Незаконный оборот криптовалют.

– Совершение преступлений, связанных с правом интеллектуальной собственности.

– Хакерские атаки на объекты инфраструктуры.

– Незаконный оборот конфиденциальной информации, включая получение прибыли.

– Преступления экономического характера, совершенные с использованием цифровых технологий.

– Общеуголовные преступления, совершенные с использованием цифровых технологий.

Действующее законодательство и правоприменительная практика динамично изменяются для обеспечения устойчивости системы противодействия распространению преступности в цифровой среде. Неслучайно целый раздел Стратегии национальной безопасности РФ посвящен информационной безопасности, где современные цифровые технологии рассматриваются как инструмент для вмешательства во внутренние дела государства. Отдельное внимание уделено распространению недостоверной, ложной информации, о заведомо ложных сообщениях об угрозе совершения террористических актов, призывах к участию в массовых беспорядка [1]. С учетом складывающихся условий, уголовной и административной ответственности, к примеру за распространение недостоверной информации явно недостаточно. Требуется нормативное закрепление механизма, определяющего привлечение к гражданско-правовой ответственности собственников цифровых СМИ, с законодательным определением размера компенсации вреда, причиняемого не только конкретному лицу, но и государственным интересам в целом.

Актуальной проблемой не только научного, но и практического характера выступает определение криминологических аспектов противодействия преступности в цифровом мире, направленном на создание условий для эффективного предупреждения преступлений, совершенных с использованием информационно-коммуникационных технологий. Работа правоохранительных органов требует оптимизации и трансформации в соответствии с новыми условиями. Усложнение правоохранительной деятельности определяется структурными изменениями, связанными с созданием новых, способных противодействовать высокотехнологичной преступности подразделений. Криминологическая реальность уже сейчас требует реформы уголовного права в части трансформации базовых уголовно-правовых институтов, криминализации новых общественно опасных деяний и уточнения признаков уголовно правовых запретов [3].

Традиционные формы и методы противодействия преступности в цифровой среде не обладают необходимым потенциалом и могут лишь использоваться как второстепенные инструменты. Совокупность передовых технологических методов, основанных на математическом моделировании с использованием ресурсов ЭВМ, направленных на масштабное изучение количественных и качественных изменений преступности и целью выявления существующих и только появившихся закономерностей преступности, составляют основу системы предупреждения преступности в цифровом мире. Обработка огромного массива информации открывает новые возможности прогнозирования преступности в краткосрочной, среднесрочной и долгосрочной перспективах. Следовательно, одной из приоритетных задач выступает достижение концептуального единства и преемственности с неоклассической криминологической теорией, продуцирования и применения новых цифровых методов и инструментов, основанных на совершенно новой теоретической базе [5. С. 423–430].

По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, технологиями завтрашнего дня являются использование искусственного интеллекта в выявлении взаимосвязей злоумышленников. Как утверждают специалисты министерства, некоторые системы уже сейчас проводят биометрический анализ клавиатурного почерка пользователя или почерка движения мыши и т. д. Системы выявляют вредоносные веб-инъекции, социальную инженерию, фишинг, бот-сети, захват учетной записи, сети нелегального обналичивания денег и другие виды банковского мошенничества. В КНР разрабатывается система интеллектуального распознавания лиц, которая будет идентифицировать любого из 1,3 млрд жителей страны за 3 секунды даже при массовом скоплении населения. Компания «Лаборатория Касперского» встраивает модели машинного обучения в свои антивирусные продукты [2].

Международное сотрудничество в рамках государственной, правоохранительной, образовательной деятельности, своевременный обмен информацией о передовых формах противодействия преступности, научных достижениях, создающих основу для построения международной системы противодействия преступности. Координация совместной деятельности субъектов противодействия преступности на национальном уровне с определением прав, обязанностей, ответственности каждого и создание специализированного правоохранительного органа повысят эффективность противодействия преступности в цифровой сфере. Реалии современности определяют будущее за использованием программно-целевых методов воздействия на преступность. Программы профилактического воздействия на отдельные виды преступности реализуются на территории многих субъектов РФ и могут содержать профилактические мероприятия, предметом которых выступает цифровая преступность.

Список литературы

1. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 14.09.2022).

2. Справка по вопросу определения перечня перспективных информационных технологий для их инвестиционной поддержки и оценки информационной безопасности (федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» // Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/uploaded/files/spravka-dlya-publikatsii-na-sajte.pdf (дата обращения: 19.09.2022).

3. Капинус О. С. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13, № 1. DOI: 10.17150/2411–6262.2022.13(1).22. EDN: NZNOMN

4. Прозументов Л. М., Шеслер А. В. Криминология. Общая часть: учебник. Томск: ООО «ДиВо», 2007. С. 57.

5. Серебренникова А. В. Криминологические проблемы цифрового мира (цифровая криминология) // Всероссийский криминологический журнал. 2020. Т. 14, № 3. С. 423–430. DOI: 10.17150/2500–4255.2020.14(3).423–430.