DOI 10.47643/1815-1337_2020_11_186

КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ГРИНЬКО Сергей Дмитриевич,
кандидат юридических наук, доцент, старший преподаватель кафедры уголовно-правовых дисциплин Российской таможенной академии.
E-mail: grinko-skags@yandex.ru

Краткая аннотация. *В статье рассматриваются криминологические риски индустрии цифровых технологий и виды преступлений, совершаемых с использованием информационных технологий. На основании проведенного исследования предлагаются меры противодействия преступлениям в данной сфере.*

Abstract. *The article discusses the criminological risks of the digital technology industry and the types of crimes committed using information technology. Measures are proposed to counter crimes in this area that based on a study.*

Ключевые слова: *цифровизация, информатизация, технологии, криптовалюта, противодействие.*
Keywords: *digitalization, informatization, technology, cryptocurrency, countermeasures.*

Одной из функций криминологии является прогностическая функция, представляющая собой разновидность социального, научного предвидения в сфере не только противодействия преступности в целом, но и отдельных ее видов. Она позволяет на основе результатов наблюдений, изучения законодательной базы и определения наступления состояний, детерминирующих преступные проявления, путем моделирования либо экспертной оценки, прогнозировать свойства преступных проявлений в будущем.

В ходе криминологического прогнозирования особая роль отводится исследованию рисков современного общества, в котором проявления человеческой активности либо «сознательно генерируют, либо допускают возможность наступления неких опасных и вредных последствий» [1, с. 105].

Раскрывая криминологические риски индустрии цифровых технологий в России, следует отметить, что процессы внедрения индустрии цифровых технологий не только диктуют новые правила, но и открывают недоступные ранее горизонты развития. Речь идет о применении технологий искусственного интеллекта, суперкомпьютерных вычислений и промышленной робототехники, автоматизации и интеллектуализации процессов, поскольку на пересечении информационных технологий промышленности, они влияют на преобразования в экономике, что повышает их конкурентоспособность в мировом хозяйстве. Поэтому в последние годы принят ряд документов, правовая основа которых обеспечивает развитие цифровых технологий в России и обеспечение информационной безопасности в области государственной и общественной безопасности [2]. Так, например, для успешной реализации Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [3], принята программа «Цифровая экономика Российской Федерации». Ее целью является повышение степени информированности и цифровой грамотности населения, улучшение доступности и качества государственных услуг, повышение благосостояния и качества жизни граждан, путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий, а также безопасности как внутри страны, так и за ее пределами.

В финансовой, банковской сфере внедрение цифровых технологий и инновационных финансовых инструментов открывает новые возможности для продвижения не только финансового бизнеса и хозяйственной деятельности, но и оказывает помощь гражданам, делая удобным использование нововведений в банковской сфере и повседневной жизни.

Особого внимания сегодня требуют развивающиеся виртуальные экономические отношения, благодаря которым активно создаются различные виды электронных платежных сервисов и технологий. Именно благодаря этим преобразованиям стали активно использоваться электронные деньги, что способствовало созданию криптовалюты как разновидности цифровой валюты, защищенной криптографическим кодом. Это привело к активному развитию различных видов электронных платежных сервисов и технологий, а также использованию электронных денег, в том числе криптовалюты, которая приобрела высокую популярность и в ряде стран стала не только полноценным платежным средством, но и выступает инвестиционным активом.

Вместе с тем, стремительное развитие названных технологий может привести, а в ряде случаев и привело к проблемам уже существующим в современном мире, к которым следует отнести социально-экономические проблемы и проблемы правового характера пока еще не решенным на законодательном уровне.

Так, например, внедрение технологий искусственного интеллекта, суперкомпьютерных вычислений и промышленной робототехники, автоматизации и интеллектуализации процессов приведет к росту безработицы. Многие считавшиеся ранее профессиональными специалисты окажутся невостребованными в новых условиях и молодежь, не получившая соответствующего образования, также останется невостребованной. Такая ситуация приведет к еще большему расслоению общества и росту преступности.

Нельзя обойти стороной и проблемы миграции, кото-

рая является показателем ухудшения социально-экономических, политических и экологических условий. При этом увеличится не только внутренняя, но и внешняя миграция, а численность нелегальных мигрантов будет возрастать [4, с. 96].

Существуют высокие риски как финансового, так и криминогенного свойства, связанные с большой популярностью криптовалюты, поскольку отсутствует ее правовой статус, она не обеспечена ликвидными активами и какими-либо гарантиями государственного либо частного капитала, поэтому осуществление операций на «виртуальных биржах» несет высокий риск потери стоимости криптовалют. Ее применение в теневой экономике позволяет обеспечить неподконтрольность национальным органам власти, незаконный оборот оружия и боеприпасов, наркотических средств, психотропных и сильнодействующих веществ, легализацию (отмывания) денежных средств или иного имущества, приобретенных преступным путем, финансирование терроризма и экстремизма, увеличивает рост преступлений, совершаемых в сфере оборота виртуальных денег.

Необходимо назвать и такие виды преступлений как мошенничество и вымогательство, совершаемые в сфере оборота виртуальных денег. Вымогательство как криминальный бизнес, о чем не раз предупреждали эксперты, получило уже высокий уровень распространенности во всем мире [5, с. 24].

Нельзя сбрасывать со счетов и уклонение от уплаты налогов, так как анонимность проводимых платежей открывает широкий диапазон для «ухода от налогообложения, функционирования в теневом секторе экономики, а также повышает риски утраты валюты собственниками в случае банкротства электронных бирж по торговле криптовалютой или в результате хакерской атаки» [6, с. 127].

Внедрение информационных технологий способствовало и изменению роли части организованной преступности, занимающейся информационным криминальным бизнесом, для которой криптовалюта является средством платежа и обналичивания.

Уровень криминологической безопасности постоянно будет высоким, а для его снижения пока не выработаны эффективные механизмы обеспечения криминологической безопасности и минимизации рисков. И, как справедливо замечают некоторые авторы: «Риски и угрозы, порожденные будущей преступностью, столь велики и многообразны, что справиться с ними силами исключительно правоохранительных органов не представляется возможным» [7, с. 5].

Системная взаимосвязь между совершением преступных деяний, различающихся по объектам посягательства и способам их совершения, проявляется между традиционными видами преступности и преступностью в сфере высоких технологий. Противопоставление последних носит условный характер, так как активное проникновение информационно-телекоммуникационных технологий в общественные отношения приведет в перспективе к «информатизации» преступности в целом [8, с. 45].

Повышенная опасность деяний, совершенных с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, определена способностью оказания негативного воздействия на неопределенно широкий круг лиц.

Изучение материалов судебной практики показывает, что ресурсы виртуальной среды, например, на сайтах, в блогах или на форумах, распространение обращений путем веерной рассылки электронных сообщений и т.п., используются в целях интеграции обособленных замкнутых групп, отдельных лиц, совершающих или склонных к совершению наркопреступлений в организованные преступные группы, взаимодействие членов которых носит экстерриториальный характер [9, с. 42].

Посредством общения в форумах, социальных сетях и личной переписке происходит вовлечение новых участников в употребление наркотических средств, а также сговор на совершение преступлений в сфере незаконного оборота наркотиков [10, с. 10].

Виртуальная среда играет существенную роль в распространении криминального опыта совершения преступлений незаконного оборота наркотических средств. Например, на ресурсах сети Интернет содержатся описания способов и средств их совершения, сокрытия следов преступления, а также отчеты о совершенных преступлениях [11, с. 123]. Это предопределило необходимость осуществления мониторинга информационного пространства сети Интернет в целях противодействия преступлениям в сфере незаконного оборота наркотиков [12, с. 13].

Необходима разработка международной системы противодействия преступлениям, совершаемых с использованием информационных технологий, которая может вестись только при условии учета национальных законодательств, а также в соответствии с особенностями политических, социальных и экономических реалий всех государств мира. Приоритет должен быть на стороне использования технологических решений при минимальном участии государственных органов и широком вовлечении объединений телекоммуникационных компаний [13, с. 109].

Таким образом, по мере проникновения информационных технологий в общественные отношения, их роль в качестве среды или способа совершения преступлений будет возрастать и это следует учитывать законодателю при формулировании составов преступлений, а также необходимо включение в ст. 63 УК РФ в качестве обстоятельства, отягчающего наказание, совершение преступления с использованием информационных технологий.

Библиография:

1. Бабаев М. М. Риски как компонент детерминационного комплекса преступности: Юридическая наука и практика // Вестник Нижегородской академии МВД России. – 2018. - № 2. – С. 104-110.
2. О Стратегии научно-технологического развития Российской Федерации:Указ Президента Российской Федерации от 1 декабря 2016 г. № 642 // Российская газета. – 2016. – 1 декабря.
3. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Российская газета. – 2017. – 10 мая.
4. Пинкевич Т. В. Криминологические риски индустрии цифровых технологий в России // Криминальные реалии, реагирование на них и закон. – М., 2018. – С. 94-99.
5. Овчинский В. С., Ларина Е. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.
6. Бурыкин А. В. Криптовалюта как виртуальный инструмент: возможности и недостатки // Перспективы формирования новой экономики XXI века. – СПб, 2017. – С. 127-131.
7. Ларина Е. С. Криминал будущего уже здесь. – М.: Книжный мир, 2017. – 507 с.
8. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая угроза // Криминология: вчера, сегодня, завтра. – 2012. - № 1. – С. 45-55.
9. Поляков В. В., Кондратьев М. В. Криминалистические особенности бесконтактного способа совершения наркопреступлений // Известия АлтГУ. – 2015. - № 2. – С. 42-46.
10. Осипенко А. Л., Миненко П. В. Оперативно-розыскное противодействие незаконному обороту наркотических средств, совершаемому с использованием телекоммуникационных устройств // Вестник ВИ МВД России. – 2014. - № 1. – С. 10-15.
11. Ошлыкова Е. А. Особенности расследования незаконного сбыта наркотических средств, совершенного бесконтактным способом с использованием сети Интернет // Гражданское общество и правовое государство. Т. 2. – Барнаул: Алтайская академия экономики и права, 2015. – С. 123-127.
12. Свистильников А. Б., Руднев С. М. Мониторинг информационного пространства сети Интернет как новое направление борьбы с преступлениями и административными проступками в сфере незаконного оборота наркотиков // Вестник Тюменского института повышения квалификации сотрудников МВД России. – 2014. - № 1. – С. 13-15.
13. Халиуллин А. И. Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в контексте обеспечения принципа сетевого нейтралитета // Криминальные реалии, реагирование на них и закон. – М., 2018. – С. 106-109.