ческие риски в области нормотворческих антинаркотических инициатив государств – членов ОДКБ[1]. Также имеет место изучение криминологических рисков (риск-ориентированного подхода) применения искусственного интеллекта[2]. Поэтому представляется возможным экстраполировать положения формирующейся в настоящей время частной теории криминологических рисков на тему исследования.

Криминологические риски необходимо исследовать, так как в первую очередь это может сказаться на качестве решения задач предупреждения преступлений: картина криминальной детерминации оказывается неполной, ее оценка неточной, следовательно, профилактическая система лишается некоторых важных предпосылок повышения эффективности своих практических усилий[3], не говоря уже о том, что риски, не взятые под контроль, оставленные на свободе, быстро разрастаются и превращаются в масштабные угрозы безопасности граждан, общества, государства. В рамках темы исследования использование рисков обусловлено необходимостью построения более точных прогнозов развития наркоситуации в регионе ответственности государств – членов ОДКБ и принятия более точных с криминологической точки зрения путей решения по ее профилактике.

Теория направлена на выявление рисков по отношению к определенному виду криминальной деятельности и ее субъектов в плане обеспечения их безопасности. По мнению П.В. Тепляшина, «ее методологическая сердцевина заключается в обоснованной допустимости прямо не ожидаемых, но возможных угроз криминального характера, дальнейшей вероятности неблагоприятного развития криминогенной обстановки и неэффективности существующих контрмер»[4].

Риски-ориентированный подход должен основываться на вызовах и угрозах коллективной безопасности ОДКБ, указанных в Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года, негативно влияющих на систему коллективной безопасности, среди которых незаконный оборот наркотических средств и психотропных веществ, их аналогов и прекурсоров в указанной территории, поступающих из Афганистана, которые носят транснациональный характер и продуцируют риски.

Таким образом, представляется крайне эффективным применение частной теории риск-ориентированного подхода, которая может способствовать прогнозированию наркопреступности в регионе ОДКБ с целью изучения перспектив повышения региональной защищенности и выработки научно обоснованных предложений и рекомендаций профилактического характера.

Никульченкова Е.В.,

кандидат юридических наук, доцент
Омский государственный университет им. Ф.М. Достоевского

Детерминанты киберпреступности в России

Эпоха цифровизации, интеллектуального разума, интернет-технологий нового поколения современного общества стали непосредственной частью нашей жизни, благодаря чему мы ускоряемся в выполнении рабочих операций, мыслительных процессов, обработки информации, принятии решений и в целом нашей жизни.

Одновременно с новыми технологиями, которые, безусловно, прогрессивно улучшили жизнь в современном мире, позволили общаться в безвременных рамках вир-

[1] Тепляшин П.В. Криминологические риски в области нормотворческих антинаркотических инициатив государств – членов Организации Договора о коллективной безопасности // Наркоконтроль. 2022. № 4. С. 9.

[2] См.: Бегишев И.Р., Хисамова З.И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. № 6(12). С. 767-775; Бегишев И.Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. № 1. С. 185-201.

[3] Бабаев М.М., Пудовочкин Ю.Е. Указ соч. С. 138.

[4] Тепляшин П.В. Указ соч. С. 9.

туально с любым уголком планеты, безопасность использования таких технологий, правовые аспекты регулирования правоотношений с использованием информационных технологий и их влияние на будущую жизнь в обществе вызывают много вопросов и обращают на себя внимание многих исследователей.

Особенно актуальными становятся проблемы роста киберпреступлений (преступлений с использованием IT-технологий) и возможности общества и государства им противостоять.

Некоторые исследователи киберпреступность определяют как совокупность преступлений, совершаемых в киберпространстве (информационном пространстве) с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных[1].

В настоящее время киберпреступность вышла на профессиональный уровень, стала изощренной и превратилась в огромный бизнес, а ее объемы стали масштабными[2].

Статистические показатели преступности, по данным ГИАЦ МВД России за период 11 месяцев 2022 г., показали, что было зарегистрировано 470143 преступлений с использованием информационных технологий, из которых раскрыто 128417 – то есть около 27%, что не может не вызывать тревогу. Из этого количества преступлений больше всего – 342495 – совершены с использованием сети Интернет; 190087 – с использованием средств мобильной связи; 116295 – с использованием пластиковых карт; 26466 – с использованием компьютерной техники[3].

По нашему мнению, низкая раскрываемость киберпреступлений обусловлена во многом невозможностью установления субъекта преступления; потерпевшего (которые либо не обращаются в правоохранительные органы, либо не подозревают, что стали объектом преступления); использованием несуществующих IP-адресов, а также трансграничным характером таких преступлений.

Нераскрытая преступность, так же как и латентная, является весьма опасным явлением ввиду ее накопительного эффекта. В дальнейшем она становится криминогенным фактором, стимулирует продолжение преступной деятельности и безнаказанности[4].

Значительная часть киберпреступлений являются латентными. Зарубежные исследователи отмечают, что преступления, связанные с неправомерным доступом к охраняемой законом компьютерной информации, характеризуются высокой степенью латентности и достигают 80-85%[5].

Анализ причинности явлений и факторов, порождающих преступления того или иного вида, является важным для выявления полной криминологической картины преступности, с помощью которой можно выработать адекватные меры противодействия.

При установлении причин и условий появления и совершения тех или иных преступлений исследователи используют разную терминологию: причины и условия совершения преступлений, обстоятельства, способствовавшие совершению преступления, криминогенные факторы, детерминанты преступления.

Детерминантами преступности являются проявления криминогенного характера, порождающие преступления и создающие благоприятные условия для выполнения преступного замысла[6].

Детерминанты всегда выступают в комплексе различных причин и условий, факторов и обстоятельств, личности преступ-

[1] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1(24). С. 45-55.

[2] Lewis, James. Economic Impact of Cybercrime. Center for Strategic and International Studies (CSIS), 2018. URL: https://www.csis.org/analysis/economic-impact-cybercrime (дата обращения: 15.01.2023).

[3] Состояние преступности в России за январь – ноябрь 2022 г. МВД РФ ФКУ «Главный информационно-аналитический центр» // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/34307225/ (дата обращения: 14.01.2023).

[4] Клейменов М.П. Нераскрытая и латентная преступность: различия и сходство // Правоприменение. 2017. Т. 1. № 1. С. 106-113.

[5] Ki Hong (Steve) Chon. Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. 2018. №1. P. 66-81.

[6] Клейменов М.П. Криминология : учебник. М.: Норма, 2018. 400 с.

ника, его мотивации и психологического состояния, виктимологических предпосылок поведения потерпевшего и др.

Киберпреступность можно охарактеризовать как криминальное антисоциальное явление, возникающее в результате применения информационных технологий, продуктов искусственного разума, IT-технологий для совершения преступлений. Характерными особенностями киберпреступлений, которые значимо отличают их от иных преступных деяний, являются высокая технологичность использования IT-технологий, Интернет-пространства, компьютерной техники, мобильных гаджетов; обладание специальными познаниями в области информационных технологий; высокая латентность, скрытый характер, во многом транснациональный масштаб совершения преступлений.

Одним из детерминантов киберпреступности является недостаточная, а порой и низкая компьютерная грамотность пользователей сети Интернет, несоблюдение правил безопасной работы в интернет-пространстве и мобильных гаджетов.

Мотивы и цели у киберпреступников самые различные – корыстные и некорыстные, политические и религиозные, диверсионные и экстремистские и масса других.

Современные средства защиты от вредоносных атак и спамов в большинстве случаев не работают на опережение. Как правило, методы защиты разрабатываются после совершенных киберпреступлений, что указывает на отставание технологий современной защиты, вследствие чего риск повторного совершения преступлений остается высоким.

Опасным фактором является совершение киберпреступлений несовершеннолетними. Молодые люди способны очень быстро адаптироваться к новым знаниям в сфере информационных технологий, но не всегда правильно их используют, а зачастую и целенаправленно овладеют такими знаниями для совершения противоправных деяний.

Увеличение количества несовершеннолетних киберпреступников объясняется многими факторами. Ими движет интерес, азарт, правовой нигилизм, легкие средства наживы, а также понимание того, что в интернет-пространстве несовершеннолетний остается неузнанным и во многих случаях неуязвимым.

Таким образом, можно заключить, что сегодня мы имеем новый вид преступности – киберпреступность, детерминантами которой выступают различные объективные и субъективные факторы, развитие информационного прогресса, совершенствование способов совершения преступлений, недостаточная правовая грамотность населения в сфере безопасного использования компьютерных программ, сети Интернет и мобильных банков, отсутствие эффективных механизмов борьбы с новыми видами преступлений в сфере информационных технологий.

Дальнейшее развитие информационных технологий и переход жизни на цифровые отношения в будущем неизбежны. Соответственно, киберпреступления будут совершенствоваться и увеличиваться. Поэтому государству необходимо серьезно отнестись к киберугрозам, выработать эффективные методы своевременного выявления, пресечения таких преступных деяний и обеспечить безопасность граждан, общества и государства в информационном пространстве.

Полагаем, эффективными мерами противодействия киберпреступлениям будут являться следующие:

1) разработка более эффективных средств и методов защиты от киберпреступлений специалистами сферы IT-технологий;

2) постоянное проведение криминологического мониторинга киберпреступности и выработка предложений по их предупреждению;

3) осуществление постоянной работы с населением и несовершеннолетними в целях повышения правовой культуры и грамотности в сфере безопасного использования интернет-технологий и ответственности за совершение киберпреступлений.

Также мы солидарны с мнением о необходимости непрерывной подготовки профессиональных кадров в правоохранительных органах, обладающих достаточными компетенциями в области информационных технологий[1].

[1] Молоков В.В. Киберпреступность: анализ и региональные особенности // Вестник Сибирского юридического института МВД России. 2022. № 4(49). С. 171-175.