Кроме того, по прогнозным оценкам в предстоящей пятилетке по ст. 205 УК Республики Беларусь ожидается рост показателя количества краж, совершенных подростками. С 2021 г. к уголовной ответственности могут привлекаться граждане уже 2007 года рождения, которым исполнится на момент совершения преступления 14 лет, а по статистике с указанного года рождаемость в Беларуси возросла на 18,6 %, что повлечет за собой участие в совершении преступлений большего количества лиц.

Устойчивость высокого удельного веса краж среди всего массива подростковой преступности требует дополнительного изучения причин и условий их совершения с целью осуществления своевременной коррекции профилактической работы с несовершеннолетними.

Чаще всего ими совершаются кражи из магазинов, автомобилей, а предметом хищения являются мобильные телефоны. Кражи могут совершаться из дачных домиков в летний период, где подростки находятся на каникулах. Основными объектами посягательства в таких случаях становятся продукты питания и одежда.

Основными причинами совершения подростками преступлений против собственности являются стремление получить материальные блага нетрудовым путем, неблагополучие в семье, плохая компания, влияние посторонних лиц, отсутствие занятости во внеучебное время, отсутствие контроля со стороны родителей и педагогов за поведением детей, а также незнание несовершеннолетними мер уголовной ответственности за совершение хищения.

Последняя причина свидетельствует о наличии одной из проблем в профилактике краж – недостаточная информированность общества и освещенность требований закона СМИ. Отсутствует профилактическая информация и в социальных сетях, где несовершеннолетние проводят много времени. И речь идет в первую очередь не о проблемных подростках, с которыми профилактическую работу обязаны проводить разные государственные органы, а о тех, которые никогда не попадали в поле зрения правоохранителей.

Социальная сеть TikTok наиболее популярна у молодежи. По информации tiktok-wiki.ru у нее самая молодая аудитория. По сравнению с остальными социальными сетями подростки составляют примерно 70 % всех пользователей данной социальной сети. В контенте TikTok присутствуют видеоролики, демонстрирующие кражи мобильных телефонов, продуктов из магазинов, но практически отсутствуют ролики профилактического характера, авторами которых выступали бы компетентные госорганы.

Кроме того, вызывает беспокойство незащищенность молодого поколения от большого потока негативной информации, которая распространяется в свободном доступе сети Интернет. Обеспечение информационного здоровья несовершеннолетних должно стать одним из приоритетных направлений в деятельности государства.

Недостаточным в профилактической работе является и правовое просвещение подростков. В ходе изучения школьной программы было установлено, что основы уголовного права в школе преподаются только в 11-м классе в рамках предмета «Обществоведение», где согласно утвержденной Министерством образования программе кратко рассматриваются понятия уголовного права. Таким образом, информация об уголовной ответственности за кражи и другие преступления несовершеннолетнему доводится только лишь к 17 годам, что уже не может рассматриваться как своевременная профилактика, так как ответственность за совершение многих из них наступает с 14 лет.

Вместе с тем основная роль воспитания возлагается прежде всего на родителей. Парадоксально, но при необходимости более глубокого разъяснения своему ребенку информации, основанной на анализе существующей криминологической ситуации, в силу отсутствия собственного «уголовного опыта» родитель опять же обращается к различным источникам информации, и в первую очередь в сеть Интернет. Однако он может столкнуться с отсутствием необходимых сведений в открытом доступе, хотя там существуют многочисленные статьи и ссылки на действующее законодательство, порой требующие владения понятийным аппаратом и специальных знаний. Следовательно, чтобы эффективнее вести работу по профилактике краж с несовершеннолетними, обязательно стоит предусмотреть размещение заинтересованными государственными органами доступной и наглядной информации, основанной на анализе совершенных преступлений.

Таким образом, во избежание совершения несовершеннолетними различных преступлений с детьми должны проводиться соответствующие воспитательные мероприятия, в ходе которых им будут разъяснены все негативные последствия противоправных поступков. Вместе с тем данная работа должна проводиться на фоне хорошей информированности населения о существующей проблематике.

Результаты прогностических оценок и выводов свидетельствуют о том, что современные реалии настоятельно требуют выработки новых подходов в профилактической работе с несовершеннолетними, а для этого необходимо использовать все возможные средства и методы информирования населения, включая возможности сети Интернет.

УДК 343.4 + 342.9 + 004

Р.Н. Ключко

НОРМАТИВНЫЕ ХАРАКТЕРИСТИКИ ИНФОРМАЦИИ И ИХ ВЛИЯНИЕ НА УСТАНОВЛЕНИЕ ПРАВОВЫХ ЗАПРЕТОВ

Определение понятия «информация» как самостоятельного концепта во многом зависит от сферы научного анализа. С точки зрения права информация в виде сведений и данных является элементом информационных отношений и выступает объектом правового регулирования. При этом в нормативных правовых актах категории «информация», «сведения», «данные» понимаются как синонимичные и не дифференцируются. Тем не менее данные можно определить как совокупность знаков, формирующих представление об объектах реальной действительности, характеризующих их, а сведения – как форму представления информации.

Нормативное определение информации дано в ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон № 455-З), где под ней понимаются «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». В зависимости от категории доступа информация делится на общедоступную и ограниченную к распространению и (или) предоставлению. На нормативно-правовом уровне определяются виды информации, которые требуют специального правового режима, а также порядок ее хранения и использования, нарушение которого запрещается под угрозой применения мер правового воздействия. Ограничения на распространение и предоставление информации, конституционно-правовые основания для которых отражены в ст. 23, 34 Конституции Республики Беларусь, устанавливаются только законодательными актами Республики Беларусь в целях обеспечения безопасности и законных интересов субъектов информационных отношений различного уровня: физических и юридических лиц, общества, государства.

В соответствии с Законом № 455-З к информации, распространение и (или) предоставление которой ограничено, относятся: информация о частной жизни физического лица и персональные данные; сведения, составляющие государственные секреты; служебная информация ограниченного распространения; информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну; информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу; иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

Информация может являться предметом или средством совершения преступления, что нашло отражение в Концепции информационной безопасности Беларуси (2019 г.), которая определяет преступления в информационной сфере как предусмотренные УК преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети. Такое определение указанной группы преступлений охватывает все посягательства на информационные отношения, выступающие в качестве как основного, так и дополнительного объекта уголовно-правовой охраны.

Установление связи между характеристиками информации, влияющими на режим ее использования (оборота), и общественной опасностью деяния с ее использованием имеет значение для определения границ криминализации информационных деяний (действия или бездействия). Концепция информационной безопасности использует следующие негативные характеристики информации: запрещенная (ст. 40, 56), недостоверная (ст. 40, 45), фальсифицированная (ст. 40), незаконная (ст. 45, 55). В Концепции применительно к информации используются и иные характеристики: своевременная, полная, достоверная, общедоступная, личная, конфиденциальная, содержащая государственные секреты, ограниченного распространения, служебная, составляющая тайну, документированная, официальная, охраняемая, массовая. Уголовное и административное законодательство также изобилуют различными характеристиками информации: компьютерная, искаженная, ложная, нераскрытая, запрещенная, неполная, неточная, недостоверная. Первая из указанных характеристик информации (компьютерная) отражает форму ее объективизации (фиксации), остальные – ее свойства, характеризующие содержательное наполнение, объем. Нормы охранительного законодательства, как и регулятивного, оперируют и такими категориями, как тайна, секреты, персональные данные и др. (например, информация о частной жизни, результатах финансово-хозяйственной деятельности эмитента ценных бумаг), которые фактически так же, как и категория «нераскрытая», отражают правовой режим информации, элементом которого выступают отдельные правовые запреты.

Правовые запреты обеспечивают охрану интересов личности, общества, государства в информационной сфере как субъектов информационных отношений, объектом которых является информация, представляющая собой экономическую либо иную ценность. Под угрозой применения уголовного наказания запрещается виновное общественно опасное информационное деяние, связанное с оборотом информации, тогда как сама по себе информация не может являться общественно опасной, вредной (вредоносной), запрещенной, незаконной. Общественно опасным, вредоносным и, соответственно, незаконным и запрещенным может быть лишь деяние, совершенное с использованием информации. Причем категории «общественная опасность» и «вредоносность» деяния являются однопорядковыми, но отличающимися по значимости причиненного вреда (ущерба). Для наглядности позволим себе привести пример, свидетельствующий о том, что сама по себе информация не может являться вредной вне деяния, связанного с ее оборотом: не представляет общественную опасность (вредность, вредоносность) информация о наркотических средствах, применяемых при анестезии, которая может содержаться в клинических протоколах, предоставляться медицинским персоналом, тогда как предоставление (распространение) информации о применении наркотических средств в немедицинских целях может представлять общественную опасность.

УК устанавливает ответственность за нарушения правового режима информации, распространение или предоставление которой ограничено (ст. 177, 178, 203, 203^1, 226^1, ст. 254, 255, 356, 358, 373, 374, 375, 375^1, 407, 408 УК). Диспозиции указанных статей являются бланкетными, предмет преступления (сведения, составляющие тайну либо секреты) в них не раскрывается, и для определения его содержательного наполнения необходимо обращение к соответствующим нормативным правовым актам, закрепляющим его признаки.

Распространение заведомо ложной (недостоверной) информации признается общественно опасным деянием исходя из значимости распространяемой информации, ценности охраняемого объекта, степени причинения ему вреда (ст. 188, 227, 238, 243^2, 250, 340, 369^1, 400, 401 УК).

Общественной опасностью может характеризоваться не только информационное действие, но и информационное бездействие, которое выражается в виде несообщения достоверной и (или) полной информации (ст. 159, 204, 237, 308, 402, 406 УК).

Таким образом, те либо иные сведения сами по себе не могут быть вредоносными и общественно опасными. Общественную опасность могут представлять лишь посягательства, совершаемые в отношении определенной информации либо

с ее использованием. На наличие либо отсутствие их общественной опасности влияет целая совокупность признаков, характеризующих как содержание информации, ее правовой режим, целевое назначение, достоверность и полноту, так и само деяние, совершаемое в отношении информации либо с ее использованием, причиненный вред либо угрозу его причинения, а также мотивы, цели и даже субъект его совершения.

УДК 343.9

П.Н. Кобец

УКРЕПЛЕНИЕ СОТРУДНИЧЕСТВА ПО ПОДГОТОВКЕ КАДРОВ ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ СТРАН СНГ В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Киберпреступность является серьезной угрозой, с которой сталкивается весь мир, но эта преступная деятельность часто ошибочно рассматривается как почти невидимое онлайн-явление, а не как проблема, реальная мировая угроза. За каждой атакой киберпреступников стоит один или несколько человек в реальном физическом пространстве. Эти люди – киберпреступники – являются продуктом определенных социально-экономических условий, влияют на все виды региональной и местной киберпреступной деятельности, в которой они специализируются. Современная киберпреступность неравномерно распределена по всему миру, но сосредоточена вокруг горячих точек, предлагающих потенциальные места, откуда преступники могут нанести удар.

В этой связи важно отметить, что в начале нового тысячелетия киберпространство проходит стадию стремительного роста. Так, по имеющимся данным, озвученным зарубежными экспертами, порядка 100 тыс. вновь созданных объектов совершают подключение к сети Интернет в течение одного часа, актуализируя тем самым реальный динамизм инноваций в сфере цифровизации основных продуктов и услуг. Следовательно, с большей открытостью и взаимодействием государств приходит повышенная их уязвимость. Угроза национальной безопасности мировых держав от кибератак реальна и растет. Организованная преступность, террористы, враждебные государства – все они стремятся использовать киберпространство для достижения собственных целей. В соответствии с аналитическим отчетом 2020 г., подготовленным компанией McAfee, которая является лидером в разработке антивирусных программных систем и представляет собой влиятельный мозговой центр в мире, исследующий основные угрозы и проблематику мировой безопасности, потери мировой экономики вследствие атак киберпреступников составляют около 1 трлн долларов США в год. В представленном отчете отмечается, что широкомасштабному ущербу от преступной деятельности киберпреступников подвергается множество предприятий, работающих как в государственном секторе экономики, так и в крупном и среднем бизнесе. От атак киберпреступников также страдает большинство ведомственных веб-порталов и множество различных сетевых ресурсов предприятий малого бизнеса.

Представители современного мирового информационного сообщества должны понимать необходимость активного совместного противодействия глобальным киберугрозам и консолидировать для этой цели все имеющиеся у них усилия. В частности, это отмечал Генеральный секретарь ООН А. Гутерриш на 14-й сессии Конгресса ООН по предупреждению преступности, стартовавшей в марте 2021 г. в Киото. Конгресс ООН по предупреждению преступности – крупнейший мировой форум, в работе которого принимают участие представители многих правительств, гражданского общества и академических кругов, эксперты по уголовному правосудию. Такие встречи укрепляют международное сотрудничество в борьбе с проявлениями различных видов мировых угроз, в том числе и опасность киберпреступности.

Поскольку преступники используют ряд новейших технологий для осуществления посягательств в цифровом пространстве, обращаясь к участникам 14-й сессии Конгресса ООН, А. Гутерриш акцентировал внимание собравшихся на необходимости пресечения злодеяний, совершаемых в киберпространстве. Он также подчеркнул, что миллионы людей в период пандемии COVID-19 пострадали от злодеяний преступников, совершавших противоправные действия в киберпространстве. Как правило, жертвы киберпреступлений пользовались информационными технологиями, оплачивая коммунальные услуги и совершая необходимые покупки, а преступники использовали сложившуюся в период пандемии ситуацию, и совершали кражи личных сведений и данных жертв, в том числе и информацию об их кредитных картах, чтобы в дальнейшем совершать различные противоправные деяния.

Таким образом, отражение кибератак и борьба с ними в настоящее время стали важнейшими задачами правоохранительных органов государств – участников СНГ. Совершенно очевидно, что в современных условиях они должны сотрудничать не только для того, чтобы избегать дублирования усилий, но и для того, чтобы учиться у своих коллег в рамках Содружества, а также накапливать информационные базы данных в целях расширения возможностей для проведения необходимых расследований рассматриваемых преступлений в своих странах. Важно также сформировать правовую базу национального и международного законодательства в этой сфере и параллельно совершенствовать имеющуюся и создавать новую правовую среду для активизации совместного научно-исследовательского сотрудничества для борьбы с киберпреступностью в рамках СНГ. Нельзя не сказать и об укреплении кадров для правоохранительных органов, готовящих специалистов в области борьбы с киберпреступностью. Необходимо стремиться к тому, чтобы большинство учебных программ по подготовке специалистов в образовательных организациях МВД стран Содружества включали в себя элементы подготовки по вопросам кибербезопасности. В свете растущего международного сотрудничества между правоохранительными органами СНГ часть предложения по обучению и образованию в странах СНГ должна быть адаптирована, в частности, путем предоставления программ на национальных языках Содружества.