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.

Решение общих задач борьбы с преступностью, повышение ее результативности сегодня немыслимо без активной научной поддержки, без внедрения в практическую деятельность современных научных разработок, подготовленных специалистами ведомственных научных и образовательных организаций стран Содружества, в соответствующих ведомствах которых в настоящее время выработана и уже сложилась система научного обеспечения оперативно-служебной деятельности органов внутренних дел.

Творческие коллективы учреждений профильного образования государств – членов СНГ, как и коллективы научно-исследовательских организаций, являются непосредственными субъектами научно-исследовательской деятельности, обеспечивают внедрение результатов проведенных научных исследований в процесс подготовки и повышения квалификации правоохранителей стран СНГ. Они также должны приложить все усилия для исследования важнейших вопросов в сфере борьбы с киберпреступностью, для дальнейшей подготовки специалистов в этой области. Хороший эффект будет достигнут в том случае, если все преподаватели, участвующие в программах по специальностям в области информационных технологий, станут заинтересованы в увеличении часовой нагрузки по предметам, связанным с безопасностью информационных систем и противодействия киберпреступности; если обучение по вопросам безопасности информационных систем, адаптированное к данной области и охватывающее проблемы, связанные с цифровыми технологиями, будет проводиться во всех начальных программах в полном объеме, а приоритет – заключаться в том, чтобы элементы безопасности интегрировались в существующие курсы и соответствующим образом в более широком контексте каждой преподаваемой области; если предлагаемые шаги будут основываться на содержании образования, разрабатываемом в тесном сотрудничестве со структурными подразделениями практиков, занятых противодействием наиважнейших угроз в сфере киберпреступности.

В заключение необходимо отметить важность наращивания темпов обучения в учреждениях профильного образования курсантов, аспирантов и докторантов из стран СНГ, поскольку практика подготовки кадрового потенциала для иностранных государств была распространенным явлением в мире, использовалась в странах СССР и является значимой.

УДК 343.238

А.В. Ковальчук

НОВЕЛЛИЗАЦИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА В ЧАСТИ РЕГЛАМЕНТАЦИИ МНОЖЕСТВЕННОСТИ ПРЕСТУПЛЕНИЙ: ВОПРОСЫ, ТРЕБУЮЩИЕ ОТВЕТОВ

Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» в УК Республики Беларусь были внесены значительные изменения и дополнения. Наиболее неоднозначными с точки зрения определения законодательной логики явились следующие новеллы, касающиеся множественности преступлений.

1. Из УК исключена такая форма множественности, как повторность преступлений (ст. 41 УК), которая, однако, была сохранена в нормах Особенной части УК в числе квалифицирующих признаков составов преступлений. При этом ст. 4 УК «Разъяснение отдельных терминов Уголовного кодекса» была дополнена ч. 14^1, закрепившей понятие преступления, совершенного повторно, т. е. преступления, совершенного лицом, которое ранее совершило какое-либо преступление, предусмотренное одной и той же статьей либо статьями, специально оговоренными (указанными) в Особенной части УК. Одновременно из УК была исключена ст. 71, регламентирующая назначение наказания при повторности преступлений, не образующих совокупности.

2. В соответствии с корректировками, внесенными в ч. 1 ст. 42 УК, расширено понятие совокупности преступлений, под которой в настоящее время понимается совершение двух или более преступлений, предусмотренных различными статьями Особенной части УК либо разными частями одной и той же статьи, а равно совершение преступлений, предусмотренных одной и той же статьей, из которых одни квалифицируются как оконченное преступление, а другие – как приготовление, покушение или соучастие в преступлении, ни за одно из которых лицо не было осуждено. При этом лицо несет уголовную ответственность за каждое совершенное преступление по соответствующей статье УК.

3. В уголовный закон введены новые виды посягательств, ответственность за совершение которых предусмотрена ст. 317^2 «Управление транспортным средством лицом, не имеющим права управления», 341^1 «Пропаганда или публичное демонстрирование, изготовление, распространение нацистской символики или атрибутики», 342^2 «Неоднократное нарушение порядка организации или проведения массовых мероприятий», причем при регламентации норм об ответственности за них впервые в Особенной части УК использован признак неоднократности преступлений.

Отмеченные нововведения в УК вызвали ряд вопросов у ученых и практиков. Во-первых, закрепленное понятие совокупности преступлений пересекается с понятием повторного совершения преступления. При указанной регламентации института множественности преступлений лицо, совершившее, например, две неквалифицированных кражи подряд, ответственность за которые предусмотрена ч. 1 ст. 205 УК (при условии, что первая из этих краж окончена, а другая – нет ввиду лишь покушения на нее), будет признано лицом, совершившим кражу повторно (ч. 2 ст. 205 УК), а также лицом, совершившим совокупность преступлений, ответственность за которые предусмотрена ч. 1 ст. 205 УК и ч. 1 ст. 14, ч. 2 ст. 205 УК (покушение на совершение повторной кражи). При этом суд при назначении наказания такому лицу должен будет учесть не только правила назначения наказаний по совокупности преступлений (ст. 72 УК), но и санкцию ч. 2 ст. 205 УК, свидетельствующую о повышенной общественной опасности второго из этих деяний, поскольку таковое признается повторным и квалифицируется по указанной норме. Учитывая закрепленный в ч. 6 ст. 3 УК постулат о недопустимости двойного инкриминирования за одно и то же преступление, следует ответить на вопрос о том, имеет ли в данном случае место двойная ответственность лица за совершение им второго общественно опасного деяния.