контроль и усилия правоохранительных органов. Эта ситуация усугубляется двумя существенными параллельными событиями в области незаконного производства и изготовления: переходом от контролируемых к неконтролируемым прекурсорам и использованием «дизайнерских» прекурсоров. В связи с этим необходимо выработать такой подход, в соответствии с которым активный контроль за известными химическими веществами (которые не имеют законных применений) стал бы более реалистичным. Именно вышеуказанные химические вещества могут потенциально использоваться при незаконном производстве и изготовлении контролируемых прекурсоров или наркотических средств.

Что касается утечки фармацевтических препаратов, используемых при незаконном производстве и изготовлении СНС, ПВ, их аналогов или НПВ, таких как эфедрин и псевдоэфедрин, то укрепление законодательства в медицинской сфере, систем мониторинга и рационального назначения лекарств может привести к снижению темпов утечки.

Для повышения доступности контролируемых лекарственных средств в национальных системах здравоохранения можно было бы ввести такие меры, как электронное назначение лекарств и создание национальных систем медицинского страхования и ценообразования на основные лекарственные средства.

Успешное противодействие правоохранительных органов синтетической наркоагрессии – предупреждение и идентификация новых синтетических наркотиков – выступает ключом к осуществлению международных конвенций о контроле над наркотиками на национальном уровне.

СНС, ПВ, их аналоги, а также НПВ легко скрыть и реализовать, поскольку для производства тысяч доз может потребоваться всего несколько граммов неконтролируемого или «дизайнерского» вещества. Очень часто такие вещества перевозят с помощью национальной или международной почты, что затрудняет их перехват из-за большого количества посылок, пересекающих границы. Современные аналитические технологии позволяют повысить потенциал идентификации таких веществ.

В связи с тем что сеть DarkNet все чаще используется преступниками в качестве платформы для производства (администрирование подпольных нарколабораторий в сети DarkNet и их онлайн-контроль) и распространения синтетических наркотических средств, то укрепление потенциала правоохранительных органов в условиях цифровизации общества, в том числе создание структурных подразделений по борьбе с киберпреступлениями (например, киберполиции), выступает важным фактором в борьбе с наркопреступностью.

Международное сотрудничество на глобальном уровне имеет решающее значение для устранения возникших проблем, связанных с расширением рынка синтетических наркотиков. Такие инструменты Управления ООН по наркотикам и преступности, как UNODC Early Warning Advisory (EWA) и UN Toolkit on Synthetic Drugs, предоставляя государствам и другим заинтересованным сторонам широкий спектр электронных ресурсов, позволят преодолеть пробелы в информации, потенциале и ресурсах в целях решения проблемы незаконного производства и распространения СНС, ПВ, их аналогов или НПВ.

УДК 343.6

А.А. Чугунов

ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПОСЯГАТЕЛЬСТВА НА ЛИЧНОСТЬ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ КИБЕРТЕХНОЛОГИЙ

Под киберпреступлениями в России понимают группу общественно опасных деяний в сфере компьютерной информации, предусмотренных гл. 28 УК РФ. Однако такой подход представляется не в полной мере отражающим содержание данного понятия. В переводе с английского cyber означает «виртуальный, связанный с информационными технологиями». Фактически характер киберпреступления зависит от уровня задействованных цифровых и сетевых технологий, образа действий преступников. По нашему мнению, киберпреступления – понятие более широкое. Оно включает в себя как посягательства на установленный порядок обращения и защиты компьютерной информации и информационных ресурсов, так и преступления, посягающие на другие объекты уголовно-правовой охраны с использованием возможностей киберпространства и его технологий. Сходной позиции придерживаются и сотрудники Управления ООН по наркотикам и преступности, которые в части определения киберпреступлений делят их на кибернезависимые (те, которые существовали и без киберпространства) и резко контрастирующие с ними киберзависимые (те, совершение которых невозможно в отсутствие соответствующих технологий). Последние представляют собой деяния, совершение которых отечественный законодатель запрещает под угрозой наказания в указанной главе УК РФ.

Отсутствие универсального понятия киберпреступлений, а также общепринятых определений видов и категорий киберпреступлений затрудняет правоприменительную практику.

Выделяют три вида компьютерных преступлений: преступления против машины, преступления с использованием машины и преступления в машине. Первая группа включает преступления против конфиденциальности, целостности и доступности компьютерных данных или систем, например неправомерное использование компьютеров хакерами. Ответственность именно за эти преступления отечественный законодатель закрепил в главе «Преступления в сфере компьютерной информации». Вторая группа включает в себя традиционные виды преступлений, такие как мошенничество или незаконные азартные игры, которые благодаря использованию цифровых и сетевых технологий приобретают глобальный масштаб, а в отсутствие сети Интернет имеют локальный характер. Преступления, включенные в третью группу, связаны с незаконным контентом. В части данных преступных деяний в международной практике нет согласия об общем подходе к их криминализации. Где-то подобные действия признаются законными, где-то – уголовно наказуемыми. В различных странах в эту катего-

рию входят размещение в сети материалов сексуального, ненавистнического, террористического характера, обнародование ложной информации и пр.

Ответственность за преступления из второй и третьей групп указанной классификации в УК РФ закреплена в виде квалифицированных составов существующих преступлений или в специальных нормах. В основном это преступления, вызывающие повышенный общественный резонанс, – преступления экономического характера (предусмотренные ч. 1 ст. 171.2, ст. 185.3, ч. 1 ст. 187 УК РФ), в том числе различные виды хищений в киберпространстве (п. «г» ч. 3 ст. 158, ст. 159.3, 159.6 УК РФ), деяния экстремистской направленности (ч. 2 ст. 205.2, ч. 2 ст. 280, ч. 2 ст. 280.1, ч. 1, 2 ст. 282 УК РФ), преступления, связанные со здоровьем населения (п. «б» ч. 2 ст. 228.1, ч. 1.1 ст. 238.1 УК РФ), детской порнографией (п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2 УК РФ).

В настоящее время практически каждое преступление может быть совершено с использованием информационно-телекоммуникационных сетей из-за обширных возможностей современных технологий. Вследствие этого возникает вопрос: почему данный признак состава преступления, несомненно влияющий на уровень общественной опасности совершенного деяния, учтен законодателем не везде, где необходимо? Например, в разд. VII УК РФ, посвященном преступлениям против личности, всего в 7 % составов предусмотрен анализируемый метод (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ст. 138.1, п. «в» ч. 2 ст. 151.2 УК РФ). Столь незначительное внимание, уделенное законодателем подобному способу совершения преступления, по нашему мнению, является пробелом в законодательстве и требует скорейшего устранения. Полагаем, что использование возможностей современных технологий позволяет виновному совершать посягательства на жизнь и здоровье человека, а также причинять вред его чести и достоинству, конституционным правам и свободам.

Приведем актуальный в настоящее время пример использования сетевых технологий как способа убийства. Больной, находящийся на лечении в больнице, подключен к аппарату искусственной вентиляции легких. Жизнь этого человека зависит от стабильности работы упомянутого медицинского оборудования, так как работа легких не может обеспечить организм достаточным количеством кислорода и аппарат искусственной вентиляции легких выполняет эту функцию. Виновный посредством удаленного доступа блокирует подачу электроэнергии для конкретных приборов искусственной вентиляции легких, вследствие чего циркуляция кислорода в организме больного прекращается и создается угроза наступления смерти человека, которая может быть предотвращена только оперативным вмешательством медицинских работников. Принятие мер по спасению жизни врачами при этом не гарантирует отсутствие причинения определенного вреда здоровью потерпевшего. Внесение соответствующих изменений в ст. 105, 111, 112, 115 УК РФ будет способствовать более эффективной защите охраняемых уголовным законом общественных отношений.

Активное распространение сейчас приобретает внедрение системы «умный дом». Автоматическое управление системами жизнеобеспечения облегчает быт и делает жилье более комфортным, но одновременно предоставляет преступникам шанс на совершение противоправных деяний, посягающих на права человека. В частности, неправомерное подключение к системе «умный дом» может нарушать права на неприкосновенность частной жизни или жилища. Например, подключение к защитной системе видеонаблюдения, призванной обеспечивать безопасность в отсутствие владельца, может служить отличным способом слежки за хозяином в период его нахождения дома, а внесение изменений в интеллектуальную программу распознавания лиц, которая сама открывает двери в дом, когда узнает владельца, – легкий способ проникновения в жилище помимо воли проживающего там лица. Считаем, что необходимо дополнить ст. 137 и ст. 139 УК РФ указанным признаком.

Подсчет голосов избирателей на выборах в большинстве субъектов РФ – процесс автоматический. Полагаем, что возможно включение способа воздействия на автоматизированную систему подсчета голосов в целях искажения итогов голосования в диспозицию ст. 142.1 УК РФ для более эффективной защиты политических прав человека.

Киберпреступность включает в себя как новые общественно опасные деяния, выделенные российским законодателем в отдельную главу Уголовного кодекса, совершение которых возможно только в связи с существованием информационно-телекоммуникационных технологий, так и традиционные преступления, совершение которых облегчает использование таких технологий. Киберпространство является неотъемлемой частью современного мира, делающей существование человека более комфортным, но в то же время предоставляющий широкие возможности для совершения различных преступлений.

Для систематизации отечественного уголовного законодательства и дифференциации ответственности за преступления, совершенные с использованием информационно-коммуникационных технологий, считаем необходимым включить анализируемый признак в квалифицированные составы преступлений против личности.

УДК 343.911

В.С. Шабаль

ЧТО ЕСТЬ ПРОФЕССИОНАЛЬНАЯ ПРЕСТУПНОСТЬ?

В обыденном понимании простого человека слово «профессиональный» отождествляется с деятельностью, которая выполняется надлежащим способом с определенным опытом. Применительно к преступности данный термин имеет немного другое значение.

В науке профессиональная преступность практически не находит своего отражения, хотя для деятельности практических органов имеет особо важное значение. В Республике Беларусь профессиональная преступность изучается в разрезе