получает «товар», владеть, пользоваться и распоряжаться которым может при наличии у него сведений об определенном наборе символов. Но криптовалюта лишена своей вещной составляющей, она существует только лишь виртуально (аппаратный криптокошелек не принимается во внимание в связи с тем, что в рассматриваемом контексте интерес представляет лишь количество криптовалюты, хранящейся на нем, а не непосредственно устройство).

Итак, вывод: криптовалюту можно приравнять к имуществу, а хищение криптовалюты путем модификации компьютерной информации следует квалифицировать по ст. 212 УК. Данный вывод сделан путем расширенного толкования, проведения аналогий, тогда как в действующем законодательстве он не нашел своего закрепления.

Существующий пробел в нормативно-правовом регулировании имущественного оборота криптовалюты создает почву для нарушения интересов пользователя в обладании данным электронным средством обмена.

Учитывая, что задача уголовного закона сводится к защите прав и свобод человека и гражданина, полагаем, что отсутствие законодательного закрепления статуса криптовалюты недопустимо. Очевидно, что расширение представлений о предмете преступного посягательства в преступлениях против собственности социально обусловлено и необходимо не только с позиций защиты законных интересов граждан от посягательств на принадлежащие им блага.

Можно отметить, что законодатель, исследователи при определении понятия «имущество» не могли предвидеть саму возможность существования имущества в каком-то нематериальном, отличном от предметов внешнего мира, виде. При этом все приведенные позиции, относительно сути определения понятия «имущество», актуальны до настоящего времени, устарело только лишь содержание физического признака. Для устранения существующих противоречий необходимо законодательно закрепить понятие «имущество». При этом под имуществом следует понимать любое благо, которое имеет экономическую ценность, признается объектом экономического оборота – принимает товарную форму, имеет стоимостное выражение, может выражаться в электронном цифровом виде.

УДК 343.985

А.А. Чехович

НЕКОТОРЫЕ АСПЕКТЫ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Развитие современного общества характеризуется повсеместным распространением информационно-коммуникационных технологий и активным развитием киберпространства. Ключевым явлением в развитии информационной сферы стало появление персональных компьютеров, а в последующем, в конце XX в., появление компьютерных сетей, в том числе сети Интернет. Благодаря компьютерным сетям финансовая, торговая, промышленная, правоохранительная и другие сферы деятельности вышли на качественно новый уровень. Сеть Интернет не только предоставила людям возможности мгновенной, непрерывной и недорогой связи по всему миру, но и стала всеобъемлющим информационным ресурсом, не имеющим аналогов и альтернативы. Указанная сеть динамична, она постоянно изменяется, обеспечивая своих пользователей новыми технологиями доступа и вариантами обмена информацией, при этом она никому не принадлежит, а также является трансграничной. Благодаря сети Интернет появился новый способ оборота информации, ее носителями стали персональные компьютеры, переносные электронные устройства хранения и передачи информации и компьютерные сети, а отдельные виды информации трансформировались в компьютерную информацию.

Вместе с тем развитие информационных технологий открыло и новые возможности для совершения преступлений с помощью персонального компьютера, как при совершении традиционных преступлений, например, мошенничества, фальшивомонетничества, незаконного оборота наркотиков, так и при совершении принципиально новых, ранее неизвестных обществу противоправных деяний – киберпреступлений.

К числу общественно опасных и латентных киберпреступлений, связанных с нарушением компьютерной безопасности, относится несанкционированный доступ к компьютерной информации, ответственность за который предусмотрена ст. 349 Уголовного кодекса Республики Беларусь. Его общественная опасность в значительной степени предопределяется использованием цифровых технологий для совершения многих других умышленных преступлений, в том числе тяжких и особо тяжких.

Необходимо отметить, что сложность раскрытия преступлений в сфере компьютерной безопасности, в частности несанкционированного доступа к компьютерной информации обусловлена рядом причин:

быстрое старение компьютерных знаний и навыков (новые образцы компьютерной техники и программного обеспечения появляются настолько быстро, а число фирм-производителей так велико, что даже специалисту трудно уследить за нововведениями);

информационные процессы протекают с очень высокими скоростями, что отрицательно сказывается на сборе доказательств;

преступления в сфере компьютерной безопасности могут совершаться специалистами в этой области знаний, что обусловливает наличие определенного уровня противодействия;

несовершенство законодательной базы, регулирующей отношения в сфере оборота информации.

В этой связи в настоящее время правоохранительная практика стала нуждаться в разработке научно обоснованных рекомендаций по совершенствованию деятельности по выявлению и пресечению несанкционированного доступа к компьютерной информации.

Высокотехнологичный характер совершения преступлений против компьютерной безопасности значительно осложняет не только их раскрытие, но и квалификацию. Как в теории, так и в практике применения ст. 349 Уголовного кодекса Республики Беларусь существуют проблемные аспекты. При применении термина «компьютерная информация» допускается неверное его толкование, не соответствующее действительности представление о значении правовых последствий. Присутствует неоднозначность при определении места совершения преступлений данного вида.

Существует необходимость анализа практики противодействия несанкционированному доступу к компьютерной информации как в Республике Беларусь, так и за рубежом, в том числе государствах, являющихся стратегическими партнерами Республики Беларусь в области противодействия киберпреступности и правоохранительной сферах. Имеется также потребность в теоретическом обосновании и определении содержания оперативно-розыскной характеристики несанкционированного доступа к компьютерной информации. Не менее востребованным представляется исследование вопросов, касающихся способов и обстоятельств совершения несанкционированного доступа к компьютерной информации.

Развитие теории оперативной-розыскной деятельности детерминирует потребность обращения к проблеме проведения отдельных видов оперативно-розыскных мероприятий, не характерных для получения информации о лицах, совершивших несанкционированный доступ к компьютерной информации. В целях наиболее полного и всестороннего установления обстоятельств несанкционированного доступа, целесообразна систематизация возможных оперативно-розыскных ситуаций, их определения на первоначальном и последующем этапах раскрытия преступления.

Решение обозначенных проблемных аспектов представляется в разработке научно-практических рекомендаций по документированию несанкционированного доступа к компьютерной информации, предложений о направлениях совершенствования оперативно-розыскной деятельности и законодательства в данной области, а также необходимостью научной разработки отдельных аспектов выявления и фиксации преступной деятельности при несанкционированном доступе к компьютерной информации.

Таким образом, вопросы оперативно-розыскного противодействия несанкционированному доступу к компьютерной информации требуют в настоящее время комплексной научной проработки, в связи с наличием ряда проблем теоретического и прикладного характера.

УДК 343.985

О.Б. Шалагинова, Н.П. Мазанов

ИННОВАЦИОННЫЕ ПОДХОДЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Целью исследования являются обоснование и разработка подхода к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность», актуального на сегодня и основанного на повышении качества усвоения учебного материала дисциплин, предусмотренных учебным планом. Эта проблема требует решения в ближайшее время, так как речь идет о завтрашнем дне России и ее национальной безопасности.

Для достижения поставленной цели предлагается использовать инновационные методы обучения, основанные на использовании современных интерактивных образовательных технологий.

Исследование основано на анализе и использовании материалов исследований в области применения педагогических технологий в современном образовательном процессе, требований законодательства, которые являются обязательными при реализации основных образовательных программ высшего профессионального образования. При подготовке статьи также были использованы материалы, полученные ав-