о системе эмиссии (децентрализованная или централизованная);

системе осуществления транзакций (открытые или анонимные);

средствах регистрации и учета в системах криптовалют и криптобирж (предусмотрена ли возможность хранения о регистрационных данных, транзакциях и IP-адресах пользователей или нет);

правовой и организационной структуре систем криптовалют и криптобирж (юридическое лицо, его филиалы, их расположение и расположение серверов);

порядке осуществления обмена, взимания комиссии, средств учета в системах криптовалют и криптобирж;

порядке регистрации и использования криптокошельков;

блокчейн-обозревателях, позволяющих получить доступ к сведениям о проведенных транзакциях той или иной криптовалюты;

признаках микширования транзакций.

Приведенные признаки и характеристики криптовалют позволяют установить, является ли цифровой знак (токен) криптовалютой, а также получить и зафиксировать криминалистически важную информацию для расследования.

В настоящее время УК прямо не предусмотрены составы преступлений, где бы в качестве исключительного предмета или средства совершения преступления выступала криптовалюта. Среди преступлений, предусмотренных главами УК, следует выделить те, где криптовалюта может рассматриваться как предмет и платежное средство преступлений:

против собственности (вымогательство, мошенничество, хищение с использованием компьютерной техники);

против порядка осуществления экономической деятельности (легализация («отмывание») средств, полученных преступным путем; приобретение либо сбыт материальных ценностей, заведомо добытых преступным путем);

против информационной безопасности (несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией);

против интересов службы (получение взятки, дача взятки).

Таким образом, полученная криминалистическая характеристика криптовалюты открывает перспективы разработки криминалистической характеристики рассматриваемых преступлений и, соответственно, методик расследования преступных деяний, предметом или платежным средством совершения которых является криптовалюта.

УДК 343.9

Е.В. Михайлова, кандидат юридических наук, преподаватель кафедры криминологии Московского университета МВД России им. В.Я. Кикотя
kis-01@mail.ru

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ НЕСОВЕРШЕННОЛЕТНИМИ: ЗАРУБЕЖНЫЙ ОПЫТ

Современные информационные технологии – неотъемлемая часть всех сфер жизнедеятельности личности, общества и государства. Однако, наряду с положительными достижениями, сфера компьютерных технологий повлекла за собой негативные последствия, в том числе увеличение количества преступлений с использованием информационно-телекоммуникационной сети Интернет, позволяющей безнаказанно совершать традиционные преступления (кража, мошенничество, вымогательство), а также неизвестные ранее мировому сообществу виды общественно опасных посягательств (неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ).

Количество пользователей сетью Интернет во всем мире стремительно увеличивается, что определяет постоянный рост размера причиняемого ущерба. По объему потенциального ущерба аналитики Всемирного экономического форума ставят киберпреступность на седьмое место в списке основных глобальных рисков: она опережает техногенные экологические катастрофы и распространение инфекционных заболеваний.

Эксперты международной консалтинговой фирмы Accenture утверждают, что в 2018 г. кибератаки в среднем обошлись одной компании в 13 млн долл., что на 12 % дороже, чем в 2017 г., в 2018 г. общие потери мировой экономики из-за действий хакеров составили 1,5 трлн долл., а в 2019 г. эта сумма выросла до 2,5 трлн долл. В соответствии с ежегодным отчетом «Hi-Tech Crime Trends 2018» каждый месяц в России успешно атакуют 1-2 банка, средний ущерб от кибератаки – 132 млн р., ущерб экономике Российской Федерации в 2018 г. составил свыше 1,1 трлн р.

И если за организацией целевых атак на банки или иные организации, как правило, стоят опытные люди, обладающие специальными знаниями, то противоправные действия в отношении физических лиц

совершают лица, не обладающие особыми знаниями в сфере компьютерных технологий, в том числе подростки. В соответствии с результатами исследования кибербезопасности «Threat Zone 17/18: новые вызовы цифрового мира», от 30 % до 40 % киберпреступлений совершаются подростками в возрасте от 14 до 16 лет.

По словам экспертов по кибербезопасности, малолетние хакеры в настоящее время представляют реальную угрозу. «Многие преступные сообщества сегодня занимаются тем, что рекрутируют таких интернет-умельцев в свои ряды. Сейчас почти каждый ребенок вырастает с компьютером в руках. И технологии, которые они осваивают, далеко не всегда мирного назначения. Как правило, все начинается с каких-то шалостей – «на спор», ради хулиганства или самоутверждения. Однако потом это перерастает в нечто более серьезное. В дальнейшем они ломают сайты корпораций или потрошат банкоматы».

Действительно, если для школьников 14–15 лет характерно совершение преступных деяний из любопытства, желания испытать острые ощущения, приобщиться к виртуальному обществу, субкультуре, то подростки старшего возраста (16–17 лет) ищут возможности заработка, в том числе путем противоправных действий (переводы денег с чужого виртуального кошелька, взломы аккаунтов в соцсетях с целью шантажа, мошеннические схемы, создание вредоносного программного обеспечения «на заказ»).

Субъективно дети и подростки часто невероятно далеки от осознания последствий своей «сетевой жизни» и тем более от понимания правовых последствий взаимодействия с интернет-ресурсами. Их любознательность и оперативность впитывания информации на фоне отсутствия необходимого социального опыта и активных попыток переноса игровых сценариев в реальную жизнь постоянно питают почву для различных правонарушений.

Чтобы предупредить возможные риски, многие государства готовят специалистов по кибербезопасности со школьной скамьи. Так, в израильских школах с четвертого класса дети изучают программирование. Учеников, успевающих по этой дисциплине, рекомендуют к дополнительным занятиям по криптографии и кибербезопасности в сертифицированных центрах. В Великобритании проводятся ежегодные молодежные соревнования по кибербезопасности (с целью привлечения детей в 2015 г. одним из этапов соревнований стал специально разработанный уровень компьютерной игры Minecraft). Австралийское правительство с 2018 г. включило обязательное преподавание блокчейн (blockchain) и криптоалгоритмов в образовательную программу, начиная с младших классов, что позволяет дать детям финансовое и цифровое образование, а также значительно уменьшить цифровой разрыв

между детьми и взрослыми. Агентство национальной безопасности Америки открывает летние лагеря для студентов, школьников и даже воспитанников детских садов. Активно используется практика по созданию так называемых отрядов «белых хакеров» (white hacker), в которые входят школьники, хорошо владеющие информационными технологиями. Такие отряды успешно тестируют программное обеспечение на различные уязвимости. Для совершенствования навыков специалистов по информационной безопасности организуются командные соревнования CTF (Capture the flag) по информационной безопасности и системному администрированию. Крупнейшими международными соревнованиями считаются проводимые Калифорнийским университетом в Санта-Барбаре, победителем которых в 2018 г. стала команда студентов Томского государственного университета SiBears.

В 2008 г. в Республике Корея создана Международная федерация киберспорта, который в настоящее время прибрел огромную популярность во многих странах мира. По компьютерному спорту проводятся соревнования как для профессиональных спортсменов, так и для любителей, в том числе студентов и школьников. Кроме того, многие учебные заведения реализуют образовательные программы по компьютерным наукам в области игровых технологий. Так, профессиональный колледж Финляндии (Оривеси) Ahlman организует обучение по трем направлениям: «Технологии разработки компьютерных игр», «Дизайн компьютерных игр», «Киберспорт». В Республике Беларусь (Минск) открыта школа киберспортивного обучения Cyber Gaming School, а также летний лагерь для детей и подростков.

Активно развивается киберспорт и в Российской Федерации. С 2006 г. проводятся официальные соревнования для студентов, обучающихся в образовательных учреждениях высшего образования страны, а после официального признания компьютерного спорта в 2016 г. была организована Всероссийская киберспортивная студенческая лига (ВКСЛ).

Инициаторами образовательных проектов для школьников выступают коммерческие и некоммерческие организации, такие как Group-IB (образовательные программы по информационной безопасности), Акционерная финансовая корпорация «Система» («Лифт в будущее»), Samsung («IT-школа Samsung»). Программы, направленные на повышение цифровой грамотности детей, запускают и разработчики компьютерных игр (например, игра-стимулятор по изучению принципов работы искусственного интеллекта «while True: learn()» от российской студии Luden).

Однако в силу ряда причин (высокая стоимость, отсутствие образовательного центра в регионе проживания, недостаточный уровень базовых знаний) такие проекты недоступны для широкой аудитории школьников.

В целях предупреждения совершения компьютерных преступлений целесообразно заниматься правовым, информационным воспитанием детей путем внедрения в школы программ повышения компьютерной грамотности, стандартов этических норм поведения в цифровой среде, соблюдения прав других граждан, ограничений, установленных законодательством, стимулировать интерес родителей к анализу медиапродукции, предпочитаемой их детьми, осуществлять контроль за интернет-сайтами, посещаемыми ребенком, стать активными участниками в процессе воспитания норм поведения в цифровом мире.

УДК 351.745.7

А.В. Мовчан, доктор юридических наук, профессор, профессор кафедры оперативно-розыскной деятельности Львовского государственного университета внутренних дел (Украина)
movchan.anatol@gmail.com

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ ПОДРАЗДЕЛЕНИЯМИ КИБЕРПОЛИЦИИ НАЦИОНАЛЬНОЙ ПОЛИЦИИ УКРАИНЫ

Термин «компьютерная преступность» (computer crime) часто употребляется наряду с термином «киберпреступность» (cybercrime), причем нередко эти понятия используются как синонимы. Согласно Закону Украины «Об основных принципах обеспечения кибербезопасности Украины» киберпреступление (компьютерное преступление) – общественно опасное виновное деяние в киберпространстве и/или с его использованием, ответственность за которое предусмотрена Законом Украины «Об уголовной ответственности» и/или которое признано преступлением международными договорами Украины.

В разд. XVI Уголовного кодекса (УК) Украины «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи» закреплены ст. 361, 361-1, 361-2, 362, 363, 363-1, которые устанавливают ответственность за такие деяния.

Согласно данным официальной статистики, в Украине за 9 месяцев 2019 г. зарегистрировано 1 796 уголовных правонарушений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей или сетей электросвязи, в том числе:

несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи (ст. 361 УК Украины) – 1 014;

несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней (ст. 362 УК Украины) – 576;

создание с целью использования, распространения или сбыта вредоносных программных или технических средств, а также их распространение или сбыт (ст. 361-1 УК Украины) – 165;

несанкционированные сбыт или распространение информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361-2 УК Украины) – 33.

Одним из субъектов противодействия компьютерной преступности в Украине являются подразделения киберполиции Национальной полиции. В частности, основная задача Департамента киберполиции Национальной полиции Украины – участие в формировании и обеспечении реализации государственной политики по предупреждению и противодействию уголовным правонарушениям, механизм подготовки, совершения или сокрытия которых предусматривает использование электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи.

Например, в сентябре 2019 г. полицейские Департамента киберполиции Национальной полиции Украины разоблачили хакера, который за время своей преступной деятельности получил несанкционированный доступ к тысячам серверов пострадавших из более чем 100 стран мира. Полученные инструменты он использовал как для продажи данных, так и для получения доступа к банковским аккаунтам и платежным системам.

Для привлечения клиентов 29-летний житель Харькова размещал на специализированных сайтах и форумах объявления о продаже доступов к удаленным серверам. Для оплаты таких услуг использовались электронные платежные системы.

Полицейские провели несколько обысков по адресам, где проживал хакер, в результате которых были изъяты компьютерная техника, деньги и внешние носители информации. Во время предварительного осмотра техники киберполиция обнаружила активные сессии и перечень взломанных серверов с учетными данными доступа к ним. По данному факту проводится досудебное расследование, квалифицированное по ч. 2 ст. 361 УК Украины.