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.

Полицейские киберполиции также разоблачили преступную группу из пяти человек во главе с 34-летним организатором, которые в течение последних двух лет создавали и продавали в сети вредоносные технические средства, предназначенные для несанкционированного вмешательства в работу систем снабжения и учета потребленной электроэнергии. В дальнейшем эти аппаратные комплексы настраивались и использовались для блокирования работы процессора электросчетчика, в результате чего энергоснабжающие предприятия несли миллионные убытки.

Для сбыта этих устройств организатор преступной группы создал отдельный интернет-сайт. В зависимости от вида электросчетчика стоимость каждого такого технического средства колебалась от 3 до 15 тыс. гривен. Таким образом злоумышленники заработали более миллиона гривен.

Полицейские изъяли во время обыска изготовленные технические средства и оборудование для их изготовления, компьютерную технику, дополнительные носители информации, банковские платежные карточки, деньги и мобильные телефоны. По данному факту проводится досудебное расследование в рамках начатого производства по ст. 361, 361-1 УК Украины.

11 сентября 2019 г. в ходе проведения в Киеве форума «Cellebrite User Forum Kyiv 2019» специалисты компании Cellebrite и Лаборатории компьютерной криминалистики «ЕПОС» рассказали участникам конференции о своих наработках в течение последнего года и поделились лучшими практиками последних достижений цифровой криминалистики.

Как отметил на форуме руководитель Департамента киберполиции Национальной полиции Украины С. Демедюк, бороться с компьютерной преступностью государству самостоятельно трудно. Ведь технологии развиваются поминутно, а преступники постоянно совершенствуют свои схемы, чтобы максимально скрыть следы.

Сегодня преступники перестают пользоваться аналоговыми каналами связи и классическими местами для хранения информации. Все чаще они используют облачные сервисы хранения информации и абузостойкие хостинги, которые не контролируются со стороны государства.

Для киберполиции важно использовать современные высокотехнологичные инструменты для получения доказательной базы. Благодаря сотрудничеству с частными организациями полицейским киберполиции удается получать данные, которые в дальнейшем используются в качестве цифровых доказательств.

Кроме того, с помощью качественной аналитики Национальная полиция получает не только доказательства противоправной деятельности, но и выявляет новые преступления.

Для того чтобы уберечь свои данные от постороннего вмешательства, киберполиция рекомендует пользователям компьютеров:

устанавливать актуальные обновления операционной системы;

использовать исключительно лицензионное программное обеспечение;

использовать современные антивирусные программы и постоянно обновлять их;

использовать только надежные пароли (состоящие из букв, чисел и символов).

УДК 339.13

А.В. Осипов, магистр, аспирант Академии управления при Президенте Республики Беларусь
7744222@tut.by

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЦЕЛЯХ ПОВЫШЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Блокчейн – база данных, безопасность которой обеспечивается механикой распределенного консенсуса. Первой широко принятой реализацией блокчейна является биткоин, для которого база данных – просто временная книги платежей. Первоначально разработанная как технология, лежащая в основе цифровой валюты биткоин, она вскоре стала распространяться за пределы криптовалют. Некоторые ученые называют систему блокчейн «машиной доверия». Из-за использования различных криптографических методов и их децентрализованного и распределенного характера, блокчейны, по заявлению экспертов, очень устойчивы. Прозрачный, безопасный и неизменный характер блокчейна вызвал интерес как частного сектора, так и государственных органов. Количество доказательств прозрачности работы технологии «блокчейн» и пилотные проекты в данном секторе стремительно растут во всем мире, а технология уже стала применяться во всех секторах экономики и общества – от финансов до электронной торговли, продовольственной безопасности, управления и даже голосования.

Проблемы экономической безопасности и трудности координации информационных и финансовых потоков через границы и между несколькими странами, участвующими в международной торговле, затруднят усилия по цифровизации работы системы государственных закупок. Новую технологию, блокчейн, многие видят как возможный