

О.Н. Брисковская, кандидат юридических наук, ведущий научный сотрудник Национальной академии внутренних дел (г. Киев, Украина)
oksanuhka@ukr.net

ЛИЧНОСТЬ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Ежегодно киберпреступность наносит государствам и частным лицам очень большой вред. Самый распространенный вид преступления – мошенничество в сети Интернет. Чаще всего мошенники создают сайты и продают несуществующий товар, очень много преступлений, касающихся выманивания информации с банковских платежных карточек и онлайн-кредитования. Преступников привлекает скорость, удобство, анонимность интернета и отсутствие границ.

Несмотря на имеющиеся в научной литературе наработки о личности преступников, их недостаточно для формирования целостного, завершенного и полного представления о личности интернет-мошенника, и возможности учета его поведенческих проявлений в процессе расследования таких преступлений. Выделение типовых моделей разных категорий преступников, знание основных черт этих людей позволяет оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск преступника и точнее определить способы установления и изобличения конкретного правонарушителя. Криминалистическая характеристика киберпреступлений отличается от уже известных криминалистической науке преступных посягательств определенной спецификой. В первую очередь в нее должны входить криминалистически значимые сведения о личности правонарушителя, мотивации его преступного поведения, типичные способы, предметы и места посягательств. Мошенники являются хорошими психологами и знают, на какие слабые стороны человеческой природы можно нажать, чтобы убедить жертву добровольно расстаться с деньгами (малообразованность, жадность, вера в «счастливый случай», жажда «халявы», лень, азарт, тщеславие, несамостоятельность, предрассудки, привычка быть вежливым и соблюдать общественные нормы, ритуалы и традиции, комплексы, невротические состояния и т. д.). Перечислим самые популярные способы на сегодня, которыми интернет-мошенники обманывают людей на покупках в сети Интернет:

схема первая – звонок из банка. Мошенники под видом покупателя звонят продавцу, некоторое время торгуются, потом берут номер бан-

ковской платежной карточки, обещая перевести средства, и несколько дней не звонят. Затем звонит «представитель банка» и сообщает, что карточка продавца, якобы была заблокирована для поступления средств от юридических лиц. Чтобы разморозить счет, мошенники предлагают воспользоваться мобильным приложением и выведывают все данные с банковской платежной карточки жертвы;

схема вторая – мошеннический сайт. Более изобретательные мошенники открывают собственные интернет-магазины. Расходы мизерные – сделать сайт можно за несколько тысяч гривен, зато нажать на нем можно чуть ли не на миллионы гривен. Если лицо заинтересовал определенный товар, его цена, стоимость которого значительно ниже, чем реализуется в других магазинах, то, конечно, лицо интересуется этим товаром, звонит мошенник, он, как правило, просит осуществить предварительно оплату 10, 20, 50 % за несуществующий товар. Или интернет-мошенники делают копию сайта банка, клиент вводит логин (номер телефона) и пароль, как следствие, их получает злоумышленник. Далее приходит sms, что доступ якобы заблокирован, звонит «сотрудник банка» и просит продиктовать код из сообщения. Логин-пароль вор уже знает и код с sms – последнее сведение, чтобы войти в настоящий аккаунт;

схема третья – деньги начислены. Например, вы продаете планшет, игровую приставку или иной товар. Мошенник договаривается с вами о встрече, вдруг сообщает, что не может на нее прийти и предлагает отдать товар его товарищу или курьеру, но после того, как на счет поступят деньги. Вам приходит sms с сообщением о начислении средств, но не от банка, а от обычного частного номера. В большинстве случаев курьером оказывается водитель маршрутки или таксист. Он спешит ехать, и вы, торопясь, отдаете товар уезжающему курьеру.

Интернет-мошенники имеют устойчивую подсознательную антисоциальную направленность. Как правило, в эту категорию входят лица, которые неоднократно совершали такие преступления. По содержанию ценностно-ориентационной направленности это преступники с корыстной направленностью, посягающие на основное достояние общества, – распределение материальных благ в соответствии с мерой и качеством затраченного труда. Мотивация интернет-мошенников – желание «легких денег», стремление к наживе. По статистическим данным, которые приводит Піцик Ю.М. в статье «Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі» в *Науковий вісник Міжнародного гуманітарного університету. Серія:*

Юриспруденція, 2017. № 26. С. 106 (105–107), большинство преступлений в интернете против собственности (79 %) – мошенничества, как правило, совершаются мужчинами (94 %), и лишь в редких случаях женщинами (6 %). Как установлено, такие преступления совершаются лицами, официально не состоящими в браке и не имеющими детей. Количество холостых лиц из общего числа составляет 70 %, в то время как в браке – 30 %. Как показывает судебная практика, 51 % лиц, совершивших преступления в сети Интернет, не имеют постоянного места работы. Среди остальных 49 % большую часть занимают менеджеры низшего и среднего звена, реже встречаются должностные лица и программисты. Так, если средний возраст мошенника в материальном мире составляет от 26 до 39 лет, то средний возраст интернет-мошенника варьируется от 18 до 35 лет. Вообще возраст интернет-мошенников может варьироваться от 18 до 45 лет, а социальное положение в обществе – от студента до сотрудника государственного учреждения или фирмы. Личностный портрет интернет-мошенника характеризуется авантюрным складом, «игровым» типом личности, в большинстве случаев постоянный риск является физиологически необходимым для мошенника, следовательно, такие лица склонны к риску, им присуща решимость, снижена тревожность, обладают самоконтролем и терпением, при этом быстро реагируют на быстро меняющуюся обстановку и легко приспосабливаются к ней. Как правило, они испытывают интеллектуальное превосходство над жертвой, уверены в себе, имеют нестандартность мышления и поведения, креативность, шарм, обаяние, настойчивость, умеют работать с информацией и быстро реагировать на изменяющуюся информацию.

С развитием интернет-технологий меняются и развиваются новые виды мошенничества в сети Интернет. Они становятся еще более опасными, так как посягают на частную, конфиденциальную информацию пользователей. С целью получения наживы интернет-мошенники используют преступные приемы, что приводит к негативным последствиям, так как их жертвами становятся не только рядовые граждане, но и частные, и государственные организации. Определение личностных свойств преступников, совершающих мошенничество в сети Интернет, позволит оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск мошенника, определять тактику ведения допроса, своевременно выявлять и расследовать такие преступления.

УДК 343.985.7:343.343.3

Н.С. Бушкевич, следователь по особо важным делам управления анализа практики и методического обеспечения предварительного расследования центрального аппарата Следственного комитета Республики Беларусь
n.bushkevich@sledcom.by

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО КАК МЕСТО АККУМУЛИРОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ О ХУЛИГАНСТВЕ

Придерживаясь традиционно-диалектического подхода в изучении причин эволюции преступности, прогнозировании тенденций и перспектив развития криминальных схем и механизмов, необходимо отметить, что одной из существенных детерминант этих процессов является внедрение в жизнедеятельность общества информационно-коммуникационных технологий.

Сегодня тренд белорусского общества – постепенный переход от традиционного индустриального общества к информационному, причем процессы цифровизации и автоматизации происходят не только на уровне отдельных индивидуумов или сообществ, когда все более совершенные девайсы, гаджеты и софты модифицируют коммуникацию между членами общества, расширяя возможности использования виртуального пространства для этих целей, но и на уровне государственно-частного партнерства. Примером является разработка ряда IT-проектов в рамках реализации стратегии государственной политики «Наука и технологии: 2018–2040», утвержденной на II Съезде ученых Беларуси в декабре 2017 г., которая предполагает переход к цифровой экономике и внедрение информационных технологий во все сферы жизнедеятельности белорусского общества.

При этом если законопослушной частью общества большинство инноваций воспринимаются с настороженностью, скептицизмом и недоверием, а процесс принятия и адаптации характеризуется продолжительностью и сложностью протекания, то преступная часть белорусского общества быстро адаптирует новые IT-возможности, вкрапляя их в механизмы достижения преступного результата, и за счет этого стремительно развивается.

Наиболее проблемным с точки зрения организации правоохранительной деятельности, направленной на защиту интересов общества и государства от противоправных посягательств, является частичный переход преступного мира в виртуальное пространство и использова-