

В число социологических теорий входят, например, ролевая теория, теория социальных достижений<sup>1</sup>.

Последователи экономической направленности пытаются объяснить появление и развитие наркопреступности в Российской Федерации прямой зависимостью от наличия на ее территории определенного рода товарно-денежных отношений. Они считают, что появление незаконного оборота наркотических средств обусловлено:

1) монополизацией внутреннего рынка, а следовательно, и возможностью получения сверхдоходов со стороны отдельных социально значимых групп;

2) наличие довольно отлаженных каналов сбыта, созданных на базе сетевого маркетинга;

3) отсутствие у наркоманов потребности приобретать иные товары, кроме самих наркотиков;

4) исключительная потребность последних в приобретении именно наркотиков;

5) реальное отсутствие у наркоманов иного способа удовлетворения этой социально-негативной потребности<sup>2</sup>.

В результате всего изложенного можно сделать следующие выводы:

1) по поводу истинного содержания причин наркопреступности в среде их исследователей отсутствует единство мнений;

2) российские криминологи пытаются объяснить их содержание на уровне трех основных направлений;

3) мы со своей стороны поддерживаем мнение тех авторов, которые, в свою очередь, считают, что по своему содержанию причины наркопреступности обладают психолого-социальным характером.

Они могут отражаться либо через криминальные установки, либо через систему психологических мотиваторов на социально-негативное поведение отдельных индивидуумов, напрямую связанное как с незаконным оборотом наркотиков, так и их потреблением не в медицинских целях<sup>3</sup>.

*Чан Тхи Вьет Ха,*

магистр

Академия народной безопасности (г. Ханой, Вьетнам)

#### **НЕКОТОРЫЕ ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В КИБЕРПРОСТРАНСТВЕ, ПРОВИНЦИАЛЬНЫМИ ПОЛИЦЕЙСКИМИ СИЛАМИ ВО ВЬЕТНАМЕ**

Мошенническое присвоение чужого имущества является преступлением, предусмотренным ст. 174 УК 2015 г. (глава о преступлениях против собственности). Под мошенническим присвоением имущества понимается «действие, направленное на использование мошеннических средств с целью присвоения чужого имущества в размере 2 000 000 донгов или более либо менее 2 000 000 донгов, подпадающее под один из случаев, предусмотренных законом». На законодательном уровне понятие мошеннических действий, связанных с имуществом, рассматривается как «действие по предоставлению ложной информации с целью создания доверия у других лиц, а также с целью передачи ими имущества и присвоения этого имущества». Мошенническое завладение имуществом осуществляется разными способами, с

использованием различных орудий и средств преступления. При этом использование киберпространства для совершения мошеннических действий и присвоения имущества является одним из популярных методов совершения преступлений в настоящее время.

Согласно ч. 3 ст. 2 Закона «О кибербезопасности» 2018 г. под киберпространством понимается «сеть соединений инфраструктуры информационных технологий, включающая в себя телекоммуникационные сети, интернет, компьютерные сети, информационные системы, системы обработки и управления информацией, базы данных, где люди осуществляют социальное поведение, не будучи ограниченными пространством и временем». Под влиянием промышленной революции 4.0, помимо положительного воздействия на общее развитие всего человечества, также наблю-

<sup>1</sup> Асмандиярова Н.Р. Криминологическая характеристика склонения к потреблению наркотических средств, психотропных веществ или их аналогов // Вестник уральского юридического института МВД России. 2018. № 3. С. 19.

<sup>2</sup> Макаров Ю.С. Незаконный оборот наркотиков // Законность. 2019. № 8. С. 43.

<sup>3</sup> Готчина Л.В. Взаимодействие правоохранительных органов по профилактике наркотизма в России // Вестник Московского университета МВД России. 2006. № 7. С. 76.

дается постоянный и стремительный рост преступлений в сфере высоких технологий. Во Вьетнаме развитие киберпространства стало «благодатной почвой» для преступников, занимающихся мошенничеством и присвоением имущества. Мошеннические преступления, связанные с незаконным присвоением собственности в киберпространстве, влекут за собой серьезные имущественные последствия и оказывают негативное психологическое воздействие на людей, а также на общую ситуацию с безопасностью и порядком.

В 2024 г. ситуация с мошенничеством и преступлениями, связанными с присвоением имущества в интернете во Вьетнаме, характеризуется следующими показателями: в августе 2024 г. по всей стране было зарегистрировано 815 случаев мошенничества и присвоения имущества, что на 11% больше, чем в предыдущем месяце, и составляет почти 16% от общего числа преступлений. Следует заметить, что почти 55% из них приходится на интернет-мошенничество. По оценкам экспертов, потери от интернет-мошенничества в 2024 г. достигнут 18 900 млрд донгов. По данным социологического опроса, 1 из 220 пользователей смартфонов стали жертвой мошенничества.

Актуальные формы мошенничества в киберпространстве во Вьетнаме сегодня:

1) выдача себя за представителя власти. В этом случае преступник звонит жертве и представляется сотрудником полиции, суда, банка либо прокурором, чтобы сообщить о том, что он участвует в деле или у него возникли проблемы с банковским счетом. После чего преступник просит предоставить личную информацию или перевести деньги для «проверки»;

2) взлом аккаунтов в социальных сетях. Хакеры взламывают аккаунты пользователей Facebook и Zalo, а затем отправляют сообщения друзьям и родственникам жертв с просьбой занять денег или запросить денежный перевод;

3) мошенничество с призами: отправка текстовых сообщений или электронных писем с информацией о том, что жертва выиграла приз с просьбой заплатить комиссию или предоставить личную информацию для получения приза, тем самым присваивая имущество;

4) выдача себя за иностранца для поиска друзей в Интернете. Преступник выдает себя за иностранца, заводит друзей через социальные сети, строит романтические отношения,

затем объявляет об отправке подарков или денег во Вьетнам и просит жертву заплатить за получение подарков, тем самым присваивая имущество;

5) мошенничество с онлайн-рекрутингом. Преступник размещает вакансии с привлекательными зарплатами, просит кандидатов оплатить обучение, купить униформу или внести депозит, а затем прекращает выходить на связь после получения денег;

6) финансовые инвестиции и мошенничество с виртуальной валютой;

7) использование технологии Deepfake;

8) выдача себя за оператора сети. Субъект выдает себя за сотрудника оператора сети, уведомляет жертву о том, что его SIM-карта будет заблокирована или ее необходимо обновить, запрашивает личную информацию или одноразовый пароль, и таким образом может завладеть банковским счетом.

9) мошенничество при онлайн-продажах: продажа товаров по низким ценам на электронных платформах или в социальных сетях после получения денег, отправки поддельных товаров, товаров низкого качества или отказа от отправки товара;

10) выдача себя за сотрудника банка для получения кредита.

С января по октябрь 2024 г. вьетнамская полиция выявила и рассматривала более 2500 случаев кибермошенничества.

На сегодняшний день преступления, связанные с мошенничеством и присвоением имущества в киберпространстве, а также практикой распределения, децентрализации и организации профилактической работы в соответствии с функциями провинциальной полиции, профилактикой преступлений в сфере мошенничества и присвоения имущества (в киберпространстве), во Вьетнаме имеют ряд особенностей.

Во-первых, предотвращение преступлений, связанных с мошенничеством и присвоением имущества в киберпространстве, требует участия и координации действий многих государственных структур, в том числе уголовной полицией. Уголовная полиция и провинциальная полиция являются органами прокуратуры и ключевыми подразделениями, непосредственно предотвращающими и пресекающими преступления, связанные с мошенничеством и присвоением имущества в киберпространстве. В соответствии с распределением обязанностей и децентрализацией профилактической деятельности существуют провинциальные подразделения уго-

ловной полиции (департаменты уголовной полиции) и группы уголовной полиции на районном уровне. При этом киберпреступность в целом и кибермошенничество в частности считаются традиционными преступлениями, совершаемыми «нетрадиционными» способами, требующими от субъектов профилактики наличия особых знаний и квалификации в области информационных технологий. Учитывая такую специфику, предотвращение вышеуказанных преступлений требует тесного взаимодействия между уголовной полицией и службами кибербезопасности, а также предотвращения и пресечения преступлений в сфере высоких технологий.

Кроме того, в работе по предотвращению преступлений, связанных с мошенничеством и присвоением имущества в киберпространстве, также принимают участие многие субъекты, использующие и применяющие результаты работы государственного управления, такие как: предприятия, предоставляющие услуги в киберпространстве, банки, агентства, организации и отдельные лица, использующие киберпространство.

Во-вторых, предотвращение мошенничества и преступлений, связанных с присвоением имущества в киберпространстве, осуществляется в неограниченной среде. Киберпространство представляет собой широкомасштабную сеть, которая позволяет одновременно участвовать большому количеству пользователей, не ограниченных пространством или временем, требуя только сетевого подключения через веб-сайты и приложения, которые в настоящее время широко распространены и доступны в использовании. Со стороны преступника киберпространство становится «источником» поиска жертв, передачи им ложной информации и совершения мошенничества и присвоения имущества.

В-третьих, положительные результаты профилактических мер, направленных на предотвращение мошеннического присвоения собственности в киберпространстве, зависят от окружающей среды, людей, подверженных риску совершения преступлений, а также людей, подверженных риску стать жертвами преступлений (субъекты профилактики).

В-четвертых, предотвращение мошенничества и преступлений, связанных с присвоением имущества в киберпространстве, требует от субъектов профилактики знаний и навыков в области информационных технологий.

Однако для профилактики имущественного мошенничества в целом и имуществ-

венного мошенничества в киберпространстве важнейшим направлением является профилактика со стороны жертв преступлений. Мошенническое завладение имуществом в киберпространстве возникает не только из-за изощренных и хитрых методов и уловок преступников, но и из-за их неосведомленности, доверчивости и других негативных психологических характеристик жертв. Поэтому профилактика данного вида преступлений должна быть сосредоточена на жертве и решениях, направленных на повышение осведомленности и навыков самозащиты, тем самым способствуя предупреждению и пресечению последствий преступлений. Для повышения эффективности профилактики преступлений со стороны жертв, в дополнение к профессиональным профилактическим мероприятиям, вьетнамской полиции необходимо уделить внимание пропаганде, распространению информации, правовому просвещению и мобилизации масс для участия в борьбе с мошенничеством и преступлениями, связанными с присвоением имущества в киберпространстве, и их предотвращении.

В первую очередь в отношении пропагандистского контента необходимо сосредоточиться на актуальных и конкретных действиях, таких как:

1) распространение правовых актов, директив, постановлений и заключений руководителей всех уровней, связанных с обеспечением кибербезопасности, борьбой с преступлениями в сфере высоких технологий, не являющимися государственной тайной;

2) изучение форм, методов и приемов преступной деятельности в киберпространстве с акцентом на их общие признаки;

3) обучение людей признакам преступлений для предотвращения и борьбы с преступлениями в киберпространстве;

4) освещение положительных результатов, достижений, личных инициатив и эффективных методов групп и отдельных лиц в борьбе с киберпреступностью.

В частности, что касается содержания методов и способов совершения преступлений, то криминальная полиция и Департамент кибербезопасности и профилактики высокотехнологичных преступлений провинциальной полиции должны координировать свои действия для разработки руководящих принципов по навыкам предотвращения преступлений мошенничества и присвоения имущества в киберпространстве:

1) быть бдительными к телефонным звонкам, информирующим о задолженности по оплате услуг стационарной связи;

2) не предоставлять личные номера телефонов, личную информацию или биографию кому-либо, не зная, кто они и для чего данные будут использоваться;

3) не покупать, не продавать, не одалживать удостоверения личности, личные счета, кредитные карты, выданные банками, а также не переводить и не вносить деньги на личные или организационные счета, не имея четкого представления о том, кто они;

4) в случае подозрения или обнаружения какого-либо лица или организации, участвующих в мошеннической деятельности, любого номера счета, запрошенного для перевода денег без законных оснований, или если счет был передан другому лицу для использования, лица обязаны немедленно сообщить в ближайший полицейский участок для предотвращения или своевременного ареста;

5) не делиться личной информацией, мыслями, чувствами и стремлениями в социальных сетях (Facebook, Zalo, Instagram и т.д.);

6) установить режим блокировки экрана, чтобы ограничить нежелательное вторжение посторонних;

7) перед утилизацией старых электронных устройств стирать персональные данные, используя методы необратимого удаления;

8) использовать оригинальное программное обеспечение от производителя, чтобы не создавать условий для проникновения злоумышленников в компьютерные или телефонные системы;

9) при использовании электронной почты на телефоне следует ограничить нажатие на вложения с ненадежных адресов электронной почты и из приложений неизвестного происхождения;

10) не предоставлять личную информацию, адрес, номер телефона, номер банковского счета людям, которых не знают;

11) не участвовать в онлайн-сайтах по инвестированию в виртуальную валюту, многоуровневом маркетинге и на сайтах с высокими процентными выплатами неизвестного происхождения.

Что касается видов пропаганды, то их необходимо усилить и разнообразить с учетом каждой местности и каждой конкретной цели. Соответственно, пропаганда должна

быть сосредоточена на таких видах деятельности, как:

– обмен полезной информацией через телевизионные программы, игровые шоу и конкурсы знаний;

– создание групп в социальных сетях с большим количеством пользователей, таких как Facebook и Zalo для оперативного обновления информации о методах и приемах преступной деятельности по мошенничеству и присвоению имущества в киберпространстве;

– размещение в киберпространстве приговоров, вынесенных судом лицам, совершившим мошенничество и присвоение имущества, с целью просвещения граждан и предотвращения дальнейших действий лиц, планирующих совершить преступления.

Что касается работы по мобилизации масс, то необходимо:

– сделать акцент на развертывании общественного движения по защите национальной безопасности, содействия внедрению моделей движения «самоуправление, самооборона, самозащита, самопримирение», повышения роли деятельности групп самоуправления, гражданской обороны, ветеранов для народа, клубов профилактики и борьбы с преступностью;

– обеспечить строительство безопасных и надежных учреждений, подразделений, предприятий и жилых районов;

– продолжить агитацию членов профсоюзов, молодежь, студентов для участия в пропаганде. Все это помогает понять, как важны соблюдение закона и бдительность в отношении способов и методов мошенничества и присвоения имущества в киберпространстве, тем самым повышая эффективность профилактики, своевременного выявления и борьбы с мошенничеством и присвоением имущества в киберпространстве;

– усилить координацию между подразделениями провинциальной полиции, включая местную полицию, отделения, профсоюзы и общественно-политические организации на местах, чтобы активизировать организацию конференций для пропаганды и распространения политики, законов;

– предоставлять широкую и своевременную информацию о новых способах мошенничества преступников в киберпространстве, чтобы каждый гражданин смог проявить бдительность, принять меры предосторожности и защитить свою собственность.