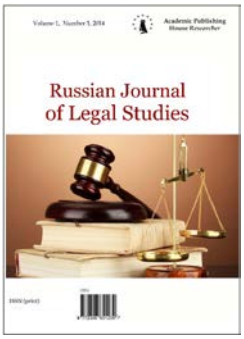
Published in the Russian Federation
Russian Journal of Legal Studies
Has been issued since 2014.
ISSN: 2409-627X
Vol. 4, Is. 2, pp. 81-87, 2015

DOI: 10.13187/rjls.2015.4.81
www.ejournal25.com



UDC 343.72

Hi-Tech Fraud: the Problems of Criminological Impact

Tetiana V. Melnychuk

National University «Odessa law academy», Ukraine
PhD, Associate Professor at the Department of Criminology and Penal Law
E-mail: t.melnychuk@onua.edu.ua

Abstract

The article deals with the problems of high-technology fraud prevention. The author outlines contemporary trends of various forms of internet banking fraud, credit card fraud, internet shopping and auction fraud, identity theft and others. The main attention is given to the description of some new approaches to criminological security of hi-tech devices using.

Keywords: high technology, hi-tech fraud, victims of fraud, fraud-monitoring, IT-security.

Введение

Инновационная функциональность преступности обусловлена дихотомией двух взаимозависимостей: «преступность стимулирует прогресс» и «преступность зависит от общественного развития».

В свое время Э. Дюркгейм указывал на парадокс феномена преступности. Хотя преступность, безусловно, приводит к некоторым дисфункциям в обществе (например, требует дополнительных финансовых затрат, наносит ущерб гражданам, приводит к социальной нестабильности), в то же время социальная функция преступности заключается в том, что ее существование (в определенных пределах) является проявлением условий, необходимых для социального развития и изменения общества. Преступность – один из факторов общественного здоровья, неотъемлемая часть всех здоровых обществ [1. С. 42].

В современных условиях все более тенденциозным становится активное использование носителями криминальной активности новейших достижений прогрессивного развития науки и техники для реализации преступных схем. Взаимосвязь преступности и развития – одна из ключевых тем 13-го Конгресса ООН по предупреждению преступности и уголовному правосудию, который состоялся в апреле 2015 года в г. Доха (Катар) [2].

Материалы и методы

Методологической основой исследования стали общенаучные и специальные методы. В частности диалектический позволил рассмотреть мошенничество в развитии и взаимосвязи с научно-техническим прогрессом, а также интерпретировать концепции и подходы к изучению hi-tech преступности в работах отечественных и зарубежных ученых. Среди специальных методов следует выделить формально-логический, сравнительно-правовой, методы системного анализа. Они способствовали достижению полноты и

достоверности исследования нормативно-правового обеспечения противодействия мошенничеству в сфере высоких технологий. Сбор эмпирического материала опосредован контент-анализом отдельных следственных документов, архивных документов суда и публикаций СМИ. На их основе исследованы современные тенденции hi-tech мошенничества и пробелы противодействия.

Обсуждение

Инновационные преобразования, сопряженные с активным развитием информационных технологий и коммуникативных связей, вносят свою лепту и в юридически значимые, правовые аспекты оценок преступности и возможностей противодействия ей. Обладающие высокой степенью адаптивности, преступные элементы из социальной реальности переходят в реальность виртуальную. Примечательно, что такие трансформации сказываются не только на экономических, но и на традиционных преступлениях, связанных с примитивными формами изъятия имущества на основе обмана либо злоупотребления доверием.

Переход к информационному обществу состоялся в контексте появления новых технологий и понимания информации как общественного ресурса. Вместе с этим аномийное состояние постсоветских сообществ, консьюмеризм, потребительская психология сформировали криминальную культуру использования информации.

Информационное общество не только порождает развитие высоких технологий (устройств, операционных и электронных коммуникативных сетей), но и делает их доступными для максимально возможного числа клиентов и пользователей, продвигая среди прочего электронную коммерцию, безналичные расчеты; соответственно в киберпространство неизбежно вовлекаются потенциальные преступники и их жертвы. Таким образом, даже традиционные, «ядерные» виды преступлений приобретают новую окраску, требуют инновационности предупредительного реагирования.

Трактовка феноменологии hi-tech мошенничества связана с содержанием термина hi-tech или «высокие технологии».

Термин «высокие технологии» находится в употреблении, начиная с конца 60-х годов. Считается, что впервые его начал использовать журналист Роберт Мец в своей авторской колонке в газете «New York Times» [3. С. 64]. Критерием отнесения технологий к высоким можно считать степень механизации процесса (или ограниченности участия человека в этом процессе).

Довольно распространенным также является употребление термина on-line мошенничество, что относится к любому типу схемы мошенничества, использующего электронную почту, веб-сайты, чаты или мессенджеры с целью отправки мошеннических предложений потенциальным жертвам, осуществления мошеннических сделок или перемещения доходов от мошенничества в финансовые или другие связанные с преступной схемой учреждения [4].

Криминологический анализ типичных механизмов совершения мошенничества с использованием высоких технологий позволяет выделить несколько его закономерностей-тенденций.

Переход от face-to-face к виртуальному мошенничеству обеспечивает дистанционность контакта «преступник-жертва» и связан, как правило, с электронной коммерцией и обманом на потребительском рынке, мошенническими схемами торговли товарами и услугами через интернет-магазины. Наблюдается также оживление финансовых пирамид, построенных по типу пирамид Понзи, которые маскируются под трейдинговые платформы с хорошей репутацией (например, Forex), интернет-казино или предлагают якобы высокодоходные инвестиционные интернет-проекты.

Электронные устройства, а также информационно-коммуникационные сети становятся предметом либо средством мошенничества. Яркий пример – вывод средств через системы онлайн-банкинга с помощью мобильных устройств пользователей. Злоумышленники получают доступ через электронную почту пользователя, перепаролируют и истребуют денежные средства.

Анонимность hi-tech мошенничества обуславливает сложности в идентификации преступников и жертв. Во многих случаях мошенничеству предшествуют в качестве

предикатных преступления, связанные с хищением личных данных (identity theft). Способами получения информации могут быть как распространение вирусов, которые устанавливают кейлоггеры (программы, записывающие все, что набирают на компьютере), чтобы обнаружить пароли, имена пользователей и номера кредитных карт; так и ситуации, когда жертвы при обычной покупке дают конфиденциальную информацию по кредитной карте или номеру социального страхования. Подмена «личности» может также включать подмену IP-адреса. Интернет-протокол подмены используется хакерами, чтобы замести следы или получить доступ к местам, обычно закрытым для них. Цели кражи данных охватываются не только использованием личной информации для материальной выгоды, но и ее использованием для получения юридических документов, таких как водительские права, медицинский полис, паспорт и др.

Латентной зачастую остается виктимизация корпоративных жертв. Далеко не всегда банки, выявившие установку скиммингового оборудования, обращаются в полицию, поскольку опасаются за свою репутацию, рискуя отпугать потенциальных клиентов. Иногда им проще заблокировать карты и компенсировать клиентам убытки.

По сравнению с традиционными видами преступности hi-tech мошенники не оставляют традиционных следов. Часто такие преступления носят транснациональный (трансграничный) характер, когда преступник, находясь в одном государстве, совершает преступление в отношении другого. Это обязывает учитывать быстродействие, результативность и трансграничность современного мошенничества при разработке мер противодействия.

И, наконец, участие преступных группировок с сетевой организацией, предполагающей децентрализованное взаимодействие, - характерная черта мошеннических схем. Как правило, это транснациональные кардерские группировки, в которых при расследовании обнаруживаются только первые (скиммеры) и последние (дропы) звенья, не позволяющие нейтрализовать целостную сеть. Карты считываются с помощью скиммера (специальное оборудование, устанавливаемое на банкомат) или внедренного в банкомат вредоносного программного обеспечения, а затем воспроизводятся на новом пластике, лицевую сторону которого оставляют белой или подделывают под карту конкретного банка. После этого дропы обналичивают чужие кредитные карты.

Так, в апреле 2014 года Министерство юстиции США выдвинуло обвинения группе хакеров в составе 9 человек за преднамеренное использование троянской программы ZeuS для сбора сведений о банковских счетах пользователей и хищении денежных средств. Перед судом предстали украинцы Юрий Коноваленко и Евгений Кулибаба, которых экстрадировали из Великобритании в августе 2012 года. Согласно обвинению, Кулибаба руководил агентурной сетью по отмыванию краденых денег на территории Соединенного Королевства. Коноваленко занимался вербовкой «дропов» и оборотом данных, украденных у жертв заражения. Четверо других подозреваемых проживают на территории Украины и России и в настоящее время остаются на свободе. Вячеслав Пенчуков предположительно осуществлял координацию действий дропов, базировавшихся в США и Великобритании, а также получал уведомления о компрометации банковских счетов. Иван Клепиков выполнял функции системного администратора и осуществлял общую техническую поддержку, Алексей Брон в качестве финансового менеджера курировал денежные переводы WebMoney, а Алексей Тихонов создавал дополнительные плагины для ZeuS. Другие члены международной киберпреступной группы не установлены [5].

Таким образом, в современном hi-tech мошенничестве наблюдается наблюдается симбиоз признаков общеуголовной корыстной преступности, киберпреступности, а также экономической с элементами организованности. Часть общественных отношений перенесена в виртуальное пространство, но вместе с этим не обеспечен контроль этого пространства и безопасность от преступных проявлений.

Одним из существенных факторов, отрицательно влияющих на возможности предупреждения, является гиперлатентность мошенничества с использованием высоких технологий. Подавляющее число преступлений остается не только нераскрытыми, но даже незарегистрированными. По некоторым оценкам, число киберпреступлений с различного рода онлайновыми платежами увеличивается ежегодно на 40–50 процентов [6].

Согласно Нортон-обзору за 2013 год, киберпреступность продолжает быть растущей глобальной проблемой. Увеличились как общие мировые прямые затраты, то есть цена киберпреступности (US $ 113 млрд; по сравнению с $ 110 млрд в предыдущем году), так и средняя стоимость киберпреступления для жертвы ($ 298; по сравнению с $ 197). Наибольший удельный вес в структуре материально выраженного вреда или 38 % занимает мошенничество [7].

По оценкам аналитиков Group-IB, за 2013 год в странах бывшего СНГ русскоговорящие хакеры заработали $ 2,5 млрд. На мошенничестве в системах интернет-банкинга, обналичивании денежных средств, банковском фишинге и мошенничестве с электронными деньгами преступники «заработали» $426 млн. На операциях по «кардингу» - $ 620 млн, распространение спама о фальшивых медикаментах и другом контрафакте, а также поддельного программного обеспечения принесло мошенникам $ 841 млн. Продажа трафика, эксплоитов, загрузок, предоставление услуг по анонимизации и прочие C2C услуги обеспечили киберпреступникам финансовый приток, равный $288 млн, на DDoS-атаках интернет-воры «заработали» $113 млн, а прочие мошеннические операции принесли им еще $153 млн [8].

Переход в киберпространство и транснациональность также ограничивает круг предупредительных возможностей на уровне отдельного государства. «Дальность» мер противодействия ограничена юрисдикцией, соответственно ограничены возможности правовой оценки действий преступников и пределы компетенции уполномоченных органов. Кроме того, нужно учитывать и фактор устойчивости группировок, который определяется их способностью противодействовать расследованию и влиять на принятие тех или иных официальных решений в области уголовной юстиции. В абсолютном выражении транснациональная организованная преступность сконцентрирована в самых богатых странах, но ее доля в общей экономике этих стран не настолько значительна, чтобы создать прямую угрозу национальной безопасности. Но когда преступные синдикаты функционируют в странах с более слабой экономикой, они способны существенно воздействовать на местные органы управления или даже контролировать правоохранительные органы [9].

Мобильный Интернет создает виртуальные связи между потенциальными жертвами и исполнителями on-line мошенничества, физически расположенными в любой точке мира, что значительно усложняет, а иногда делает невозможным процесс идентификации, парализует расследование. Механизм таких преступлений порой исключает возможность понимания их истинной распространенности, особенно в виду неочевидного для многих жертв и неосознаваемого до определенного момента процесса виктимизации. Кроме того, удаленный доступ к отдельным компьютерам и их сетям создает сложности в установлении «фактического места» совершения преступлений и таким образом определения юрисдикции следствия и правосудия.

Инновационность и техничность функционирования групп формируют новые, постоянно модифицирующиеся виды мошенничества, что делает его «движущейся мишенью» и приводит к усилению отставания социально-правового контроля. Такие группы и их деятельность низко чувствительны к предупредительным мерам. В то время как мошенники работают на опережение (у них лучшая техническая оснащенность, более высокой темп и квалификация в предметной области), потерпевшие от мошенничества вынуждены подавать письменное заявление по месту жительства. Правоохранительные органы «связаны» необходимостью действовать согласно официальным процессуальным требованиям и использовать традиционные подходы.

Необходимым условием результативного выявления hi-tech мошенничества, привлечения виновных к ответственности, возмещения ущерба является криминализация данных деяний на национальном уровне. Если в уголовном кодексе какого-либо государства не предусмотрена ответственность за такие деяния, то это государство превращается в «правовую крышу» для киберпреступников.

Вместе с этим при формальном наличии необходимых уголовно-правовых норм о киберпреступлениях, проблемы с закреплением противоправности и наказуемости hi-tech преступных схем остаются. Это обусловлено динамичностью и инновационностью мошеннических действий с использованием высоких технологий. Специфика преступлений

в этой сфере такова, что законодательство всегда отстает, а новые деяния надлежащим образом не охватываются существующими диспозициями. Анализ следственной практики по таким делам в Украине показывает, что для квалификации, как правило, используются ст. 190 (мошенничество), ст. 200 (незаконные действия с документами на перевод, платежными карточками и другими средствами доступа к банковским счетам, электронными деньгами, оборудованием для их изготовления) и ст. 231 (незаконный сбор с целью использования или использование сведений, составляющих коммерческую или банковскую тайну) Уголовного кодекса Украины.

Определение характерных криминологических признаков позволит усовершенствовать квалифицирующие признаки и конструкцию составов с тем, чтобы уголовное право могло выполнять охранительную функцию. Составы должны отвечать криминогенной обстановке, использовать бланкетные нормы, не ограничивающие сферу высоких технологий. Кроме того, требуют пересмотра санкции в зависимости от размера ущерба, также некоторые базовые признаки составов, в частности высказываются предложения о снижении возраста ответственности до 14 лет [10. С. 7].

Перспективный аспект реагирования на hi-tech мошенничество состоит в применении специализированных мер противодействия. Технологичности мошеннических схем должны отвечать новые технологии обеспечения криминологической безопасности коммерческих расчетов, пользования электронными устройствами и прочее, ограничивающие или нейтрализующие саму возможность мошенничества. Так, формой противодействия мошенничеству в сфере банковско-кредитной деятельности, активно используемой банками развитых стран, является так называемый фрод-мониторинг информации, полученной банковским учреждением при ведении бизнеса [11]. Фрод-мониторинг базируется на определении поведенческой модели пользователя и формальных (статических) правил. В случае с инсайдером (сотрудником банка) речь идет о модели работы сотрудника в соответствии с должностной инструкцией. Кроме того, корпоративным субъектам следует заботиться об IT-безопасности (защита от Ddos-атак, защита рабочих мест и информационной инфраструктуры предприятия, защита мобильного и он-лайн-банкинга и др.).

Учитывая то, что не смотря на всю «хайтековость» мошенничества неизменным в детерминации остается человеческий виктимологический фактор, не утрачивает актуальности и виктимологическая профилактика, связанная с информированием о рисках обмана или злоупотребления доверием и обучением нормам безопасного поведения при покупках в интернет-магазинах, пользованием электронными устройствами или передачей персональных данных. В последнее время в Украине наряду с традиционным hi-tech мошенничеством появилось мошенничество с применением методов социального инжиниринга. Преступники переключаются на применение психологических приемов под видом волонтеров, заботящихся о вынужденных переселенцах и участвующих в боевых действиях, «давят» на патриотизм и сочувствие, в результате которых пострадавшие самостоятельно и добровольно перечисляют свои средства мошенникам. Элементарная осмотрительность и проверка информации могли бы позволить избежать виктимизации.

Заключение

Прогрессивное развитие современных общественных отношений неизбежно связано с разработкой и внедрением высоких технологий в различные сферы. Все более популярной становится концепция Интернета вещей, но вместе с новыми технологиями появляются и новые риски [12], имеющие криминологическую природу и влекущие деструктивные последствия. Это актуализирует внедрение систем криминологической безопасности и усовершенствование уголовно-правового воздействия.

Примечания:

1. См. Дюркгейм Э. Норма и патология / Э. Дюркгейм // Социология преступности. М., 1966.

2. Официальная страница Конгресса [Электронный ресурс] – URL: http://www.un.org/ru/events/crimecongress2015/index.shtml.

3. Metz R. Market Place: Keeping an Eye On Big Trends // The New York Times, November 4, 1969.

4. Australian Federal Police [Электронный ресурс] – URL: http://www.afp. gov.au/ policing/cybercrime/online-fraud-and-scams

5. Nine Charged in Conspiracy to Steal Millions of Dollars Using “Zeus” Malware. The United States Department of Justice [Электронный ресурс] – URL: http://www.justice.gov /opa/pr/nine-charged-conspiracy-steal-millions-dollars-using-zeus-malware.

6. Кредитка доверия // Итоги №23 / 782 (06.06.11) [Электронный ресурс] – URL: http://www.itogi.ru/hitech-business/2011/23/166012.html.

7. Norton Report 2013 [Электронный ресурс] – URL: http:/www.symantec. com/about /news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

8. Объем рынка киберпреступности в 2013 году составил $2,5 млрд [Электронный ресурс] – URL: http://www.group-ib.ru/index.php/7-novosti/1697-obem-rynka-kiberpre stupnosti -v-2013-godu-sostavil-25-mlrd.

9. См. Мельничук Т.В. Криминальные тренды: глобализация vs локализация / Т.В. Мельничук // Материалы II Международной научно-практической конференции «Актуальные проблемы криминологического исследования региональной преступности» (21 октября 2014 года, Баку), 2015. С. 208-215.

10. Медведев С.С. Мошенничество в сфере высоких технологий: автореф. дис. ... канд. юрид. наук: 12.00.08 / С.С.Медведев. Краснодар, 2008. 22 с.

11. См.: Рогожнікова Н.В. Концептуальні підходи до моніторингу як форми спостереження за процесом споживчого кредитування в комерційному банку / Н.В. Рогожнікова // Вісник Університету банківської справи Національного Банку України. – 2010. № 3 (9). С. 74; Мітрічев І. Фрод-моніторинг для протидії шахрайству в банківських установах [Электронный ресурс] // Україна Фінансова – URL: http://ufin.com.ua /analit_ mat/sdu/131.htm (дата обращения: 1.06.2015).

12. См. Gan Gang, Lu Zeyong, Jiang Jun. Internet of Things Security Analysis // Internet Technology and Applications (iTAP), 2011 International Conference, 2011. P. 1-4.

References:

1. See: Dyurkgeim E. Norma i patologiya // Sotsiologiya prestupnosti. M., 1966.

2. Ofitsial'naya stranitsa Kongressa [Elektronnyi resurs] – URL: http://www.un.org /ru/events/crimecongress2015/index.shtml.

3. Metz R. Market Place: Keeping an Eye On Big Trends // The New York Times, November 4, 1969.

4. Australian Federal Police [Elektronnyi resurs] – URL: http://www.afp.gov.au /policing /cybercrime/online-fraud-and-scams.

5. Nine Charged in Conspiracy to Steal Millions of Dollars Using “Zeus” Malware. The United States Department of Justice [Elektronnyi resurs] – URL: http://www.justice.gov/opa/pr/nine-charged-conspiracy-steal-millions-dollars-using-zeus-malware.

6. Kreditka doveriya // Itogi №23 / 782 (06.06.11) [Elektronnyi resurs] – URL: http://www.itogi.ru/hitech-business/2011/23/166012.html.

7. Norton Report 2013 [Elektronnyi resurs] – URL: http://www.symantec.com /about /news/resources/press_kits/detail.jsp?pkid=norton-report-2013 (data obrashcheniya: 1.06.2015).

8. Ob"em rynka kiberprestupnosti v 2013 godu sostavil $2,5 mlrd [Elektronnyi resurs] – URL: http://www.group-ib.ru/index.php/7-novosti/1697-obem-rynka-kiberprestupnosti-v-2013-godu-sostavil-25-mlrd (data obrashcheniya: 1.06.2015).

9. See: Mel'nichuk T.V. Kriminal'nye trendy: globalizatsiya vs lokalizatsiya / T.V. Mel'nichuk // Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Aktual'nye problemy kriminologicheskogo issledovaniya regional'noi prestupnosti» (21 oktyabrya 2014 goda, Baku), 2015. S. 208-2015.

10. Medvedev, S.S. Moshennichestvo v sfere vysokikh tekhnologii: avtoref. dis. ... kand. yurid. nauk: 12.00.08 / S.S.Medvedev. Krasnodar, 2008. 22 s.

11. See: Rogozhnikova N.V. Kontseptual'ni pidkhodi do monitoringu yak formi sposterezhennya za protsesom spozhivchogo kredituvannya v komertsiinomu banku / N.V. Rogozhnikova // Visnik Universitetu bankivs'koї spravi Natsional'nogo Banku Ukraïni. 2010.

№ 3 (9). S. 74; Mitrichev I. Frod-monitoring dlya protidiï shakhraistvu v bankivs'kikh ustanovakh [Elektronnyi resurs] // Ukraïna Finansova – URL: http://ufin.com.ua/analit_mat/sdu/131.htm.

12. See: Gan Gang, Lu Zeyong, Jiang Jun. Internet of Things Security Analysis // Internet Technology and Applications (iTAP), 2011 International Conference, 2011. P. 1-4.

УДК 343.72

Hi-tech мошенничество: проблемы криминологического воздействия

Татьяна Владимировна Мельничук

Национальный университет «Одесская юридическая академия», Украина
Кандидат юридических наук, доцент
E-mail: t.melnychuk@onua.edu.ua

Аннотация. Статья посвящена проблемам предупреждения мошенничества в сфере высоких технологий. Автор описывает современные тенденции различных форм мошенничества в интернет-банкинге, мошенничества с кредитными картами, мошенничества интернет-магазинов, хищения персональных данных и др. Основное внимание уделено анализу некоторых новых подходов к криминологической безопасности использования высокотехнологических устройств.

Ключевые слова: высокие технологии, мошенничество с использованием высоких технологий, жертвы мошенничества, фрод-мониторинг, IT-безопасность.