ЛЕГАЛИЗАЦИЯ ДЕНЕЖНЫХ СРЕДСТВ, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

А.В. Ширяев, О.В. Ушаков
Алтайский государственный университет, г. Барнаул

В новом докладе, приуроченном к форуму Всемирной встречи ООН на высшем уровне по вопросам информационного общества отмечается, что в период с 2000 года по 2015 год число пользователей сети Интернет увеличилось почти в 7 раз с 6,5% до 43% мирового населения [1]. Необходимо также отметить, что способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также принципиально новых или модифицированных программ [2]. Информационные технологии являются ключевым фактором для инновационного и экономического роста в последние десятилетия. Однако дальнейшее развитие технологий, в частности, сети Интернет, вызывает опасения в плане использования преступниками преимуществ, которые технологии предоставляют для осуществления незаконных действий. Результатом таких действий становится исключительно высокая латентность компьютерных преступлений [3]. В связи с этим государство стремится найти способы адаптации нормативно-правовой базы, чтобы защитить своих граждан и бизнес от преступности и ликвидировать последствия использования сети Интернет в незаконных целях. Безграничный характер информационных сетей переносит проблему регулирования на международный уровень и ставит сложную задачу по формированию надежной и безопасной онлайн-среды.

На сегодняшний день одним из наиболее распространенных видов компьютерных преступлений является хищение денежных средств со счетов клиентов банков. Хищение денежных средств с банковских карт уже не первый год является проблемой как для собственников банковских счетов, так и для кредитных организаций, в которых указанные счета открыты [4]. Однако само по себе хищение денежных средств с чужого банковского счета уже не представляется чем-то новым и высокотехнологичным, поскольку данные банковских карт возможно приобрести в Интернете на соответствующих торговых площадках. Особый интерес представляет процесс легализации похищенных денежных средств, поскольку именно на этом этапе возможно установить конечного получателя денежных средств для привлечения его к уголовной ответственности.

Кодификатор рабочей группы Интерпола в обобщенном виде компьютерные мошенничества предлагает определять и классифицировать следующим образом: 1) компьютерные мошенничества, связанные с хищением наличных денег из банкоматов; 2) компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств; 3) мошенничества и хищения, связанные с игровыми автоматами; 4) манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из них путем манипуляции программами; 5) компьютерные мошенничества и хищения, связанные с платежными средствами; 6) телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы [5].

Данные способы компьютерного мошенничества могут осуществляться на трех этапах:

1) размещение - внесение денег в финансовую систему;

2) расслоение - дистанцирование денег от источника через серию транзакций;

3) интеграция – объединение денег с фондами в легальном секторе [6].

С ростом информационных технологий, способы мошенничества значительно изменились и трансформировались. Например, цифровые сети позволяют пройти этап

размещения, потому что похищенные денежные средства уже существуют онлайн [7]. Платежные системы дают возможность быстрого разделения денег на небольшие суммы, а затем объединения небольших суммы в большие на последующих этапах, что позволяет преступникам использовать множество схем для перевода денег с многоуровневой обработкой. На этапе интеграции, модели электронной коммерции могут быть заимствованы из законного сектора для создания компаний, таких как электронные трейдеры или онлайн-казино, которые будут интегрировать преступный денежный оборот и делать его законным. Мошенничество в сфере компьютерной информации, тесно связано с киберотмыванием и организованной киберпреступностью в Интернете [8]. Интернет может быть использован для отмывания прибыли от любой незаконной деятельности.

Конвергенция различных областей, таких как, например, азартные онлайн-игры и цифровые валюты, электронные платежи, значительно усложняет процесс регулирования и контроля, так как интернет является сложной и децентрализованной структурой, где возможность отслеживания, уголовного преследования требует от сотрудников правоохранительных органов специальных знаний и слаженного международного сотрудничества. В связи с этим не всегда понятно, как обеспечить соблюдение нормативных требований в онлайн-среде и контроль со стороны государства, когда в физическом мире нет «точки продажи» [9].

Как представляется, это обусловлено небольшой наработкой судебной практики расследования данных преступлений, которые законодатель в Уголовном кодексе РФ выделил в отдельную ст. 159.6 «Мошенничество в сфере компьютерной информации» лишь с 2012 г. Федеральным законом от 29 ноября 2012 г.№ 207-ФЗ.99 [10].

В большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение [11]. Это позволяет комбинировать разные варианты и создавать новые схемы мошенничества в сфере компьютерной информации: 1) использование традиционных валют для осуществления онлайн-платежей и онлайн-переводов; 2) использование цифровых валют; 3) торговля виртуальными товарами, которая может осуществляться с использованием традиционных или цифровых валют; 4) торговля реальными товарами (включая нелегальные товары, такие как наркотики или оружие) с использованием традиционных или цифровых валют; 5) онлайн-сервисы, как легальные, так и нелегальные, использующие условные или цифровые валюты, в том числе азартные онлайн-игры.

Существует несколько основных областей в онлайн-среде, которые наиболее уязвимы для деятельности киберпреступников. Онлайн-банкинг является одним из самых известных способов компьютерного мошенничества, поскольку банки и их клиенты являются одной из основных целей для киберпреступников [12]. Легализация денежных средств, похищенных с банковских счетов, является уязвимым местом для кибермошенников, потому что в основном этот процесс осуществляется при помощи посредников, между которыми деньги можно разделить на части, быстро и легко перевести их на множество банковских счетов в разных финансовых учреждениях.

Поскольку преступные действия могут осуществляться в юрисдикциях разных стран, обнаружить денежные средства и отследить их движение очень трудно. Мобильный банкинг - явление, которое обусловлено растущим спросом на микроплатежи, осуществляемые через мобильный телефон, где операторы мобильной связи выступают в качестве финансовых посредников [13]. Возможность покупки сим-карты без регистрации и проверки личности, обеспечивает высокую степень анонимности мобильного платежа, которую кибермошенники обращают в свою пользу.

Небанковские поставщики платежных услуг, такие как «PayPal», представляют собой дешевый, быстрый и анонимный способ перевода денег на международном уровне, в том числе для оплаты товаров и услуг. Преимущество этих услуг для кибермошенников заключается в том, что есть возможность агрегирования суммы, посредством перевода очень небольших сумм денег много раз, не привлекая внимания мониторинга подозрительного поведения [14].

В отличие от обычной, цифровая валюта (или электронная валюта), является быстро растущей областью Интернета и представляет собой систему обмена ценностями, посредством транзакций, которые существуют только онлайн и не имеют отношения к финансовым организациям. Анонимность цифровых валют, безусловно, является фактором, способствующим незаконной деятельности, в частности установлено, что поставщики цифровых валют, таких как «e-gold» и «Liberty», использовались для легализации незаконных доходов [15]. Это создает неопределенность относительно того, как регулировать оборот данной валюты, так как у нее нет единой платформы.

Некоторые ученые утверждают, что азартные онлайн-игры представляют собой идеальный инструмент для компьютерного мошенничества (особенно с использованием цифровых валют или платежей, осуществляемых через нерегулируемых посредников), чтобы дистанцировать деньги от незаконного источника, легализуя их и обналичивая [16]. Данный способ компьютерного мошенничества достаточно просто реализовать, имея данные банковской карты, киберпреступники фиктивно проигрывают друг другу имеющиеся на ней денежные средства в онлайн-игры, нанося ущерб банку, с минимальными шансами обнаружить себя и похищенные денежные средства.

Интернет предлагает различные возможности для торговли легальными и нелегальными товарами, а также для обмена незаконно полученных денежных средств на товары с целью дальнейшей продажи. Это может быть частью этапа размещения или расслоения, когда незаконно полученные деньги обмениваются на определенные товары, а затем товары продаются, чтобы дистанцировать прибыль от источника. Одним из способов компьютерного мошенничества также является создание электронных коммерческих компаний, по продаже товаров, которые изначально доставлять до заказчика не планируется [17].

Конвергенция различных областей, таких как, например, азартные онлайн-игры и цифровые валюты, электронная коммерция и электронные платежи, услуги связи и банковское дело, делает систему кибермошенничества чрезвычайно сложной с точки зрения регулирования и контроля. Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений [18].

Перед органами предварительного расследования стоит сложная задача непрерывного изучения изменяющейся компьютерной преступности и выработке по ней соответствующих методик расследования, в связи с тем, что злоумышленники используют различные хитрости, камуфлируют правонарушения различными субъективными и объективными причинами [19]. Мобилизация международного сообщества, осведомленность на национальном уровне, а также совместные усилия по осуществлению и обеспечению соблюдения конкретных мер безопасности - это цели, которые информационное общество должно достичь, чтобы успешно бороться с киберпреступностью.

Библиографический список

1. Рядовский И.А. Киберпреступность: современное состояние и тенденции трансформации // Преступность в сфере информационно-телекоммуникационных технологий. Сборник статей. – 2015. – С. 24-28.
2. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации // матер. ежег. Всерос. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно-процессуальные и криминалистические чтения на Алтае». – Барнаул: Изд-во Алт. ун-та. – 2012. – №.11–12. – С.123–126.
3. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 43–46.
4. Ерошенков Н.В., Цветов В.И. Справочные интернет-ресурсы в раскрытии преступлений, связанных с хищением денежных средств с банковских счетов граждан // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2019. – № 3. – С. 29–34.
5. Вопросы международного сотрудничества в борьбе с компьютерными преступлениями. [Электронный ресурс] // URL: http://www.crime-research.ru/news
6. Tropina, T. Fighting money laundering in the age of online banking, virtual currencies and internet gambling // Article in ERA Forum. – 2014. – №. 15(1), - С.69–84.
7. Council of Europe: Moneywal report: criminal money flows on the internet: methods, trends and multi-stakeholder counteraction. 2012. [Электронный ресурс] / URL: http://www.coe.int/t/dghl/monitoring/moneyval/typologies/MONEYVAL(2010)9_Reptyp_full_en.pdf
8. European Central Bank: Virtual currency schemes. [Электронный ресурс]/ 2012. URL: www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
9. Haines, J., Johnstone, P. Global cybercrime: new toys for the money launderers // Money Laund. Control. – 1999. - No.2(4), С. 317–325.
10. Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. – 2015. – № 3. – С.145-149.
11. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АлтГУ. – 2013. – № 2. – С. 114–116.
12. Levi, M. Money-Laundering Risks and e-Gaming: a European Overview and Assessment: Final Re-port // European Gaming and Betting Association (EGBA), Brussels, - 2009. - С.2-4.
13. Piller, G., Zaccariotto, E. Cyber-laundering: the union between new electronic payment systems and criminal organizations // Trans. Stud. Rev. – 2009. - №.16(1), С. 62–76.
14. Tropina, T. Self- and co-regulation in fighting cybercrime and safeguarding cybersecurity. Current Issues in IT Security // Duncker & Humblot, Berlin, - 2012. С.155–170.
15. Weimer, W. Cyberlaundering: an international cache for microchip money // DePaul Bus. Law J. – 2000-2001. – №.13(1–2). – С.69–84.
16. Fiedler, I. Online gambling as a game changer to money laundering? [Электронный ресурс] // 2013. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2261266.

17. Weaver S. Modern day money laundering: does the solution exist in an expansive system of moni-toring and record keeping regulations? // Annu. Rev. Bank. Law Financ. Law 24. – 2005. – С. 443–465.
18. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады ТУСУРа. –2014. – № 2 (32). – С.165.
19. Ширяев А.В. Объект и предмет неправомерного доступа к компьютерной информации // Информационное противодействие экстремизму и терроризму. Сборник трудов II всероссийской научно-практической конференции: Изд-во Краснодарского университет МВД РФ. – 2015. – С.108-109.