УДК 343.9

# ПРОФЕССИОНАЛЬНОЕ КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО КАК РАЗНОВИДНОСТЬ ПРОФЕССИОНАЛЬНОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

***Людмила Валерьевна Пивнева***
Юго-Западный государственный университет, Курск, Россия,
Белгородский юридический институт МВД России имени И.Д. Путилина, Белгород, Россия
iPVmila@yandex.ru

*Аннотация.* В настоящее время с помощью новых информационных технологий можно быстро, а главное удобно, произвести разные финансовые операции в безналичной форме, в связи с чем в виртуальную среду переместились большие потоки денежных средств. Однако эти манипуляции с денежными средствами до сих пор не имеют высокой степени правовой, организационно-технической защиты. Вследствие этого информационное пространство с каждым годом все более активно осваивают не только обычные граждане, но и профессиональные преступники, чей промысел как раз и ориентирован на постоянное извлечение прибыли от совершения преступлений. В результате особую актуальность сейчас приобретают вопросы криминологической оценки деятельности отдельных категорий преступников-профессионалов, промышляющих в виртуальной сфере.

В связи с изложенным целью исследования является определение особенностей профессиональной преступной деятельности компьютерных мошенников в условиях развития информационного пространства.

В статье рассмотрены основные специализации современных компьютерных мошенников (фишеры и кардеры), определены присущие им признаки криминального профессионализма. Установлено, что они с каждым днем становятся все профессиональнее. Для противодействия этой преступной деятельности считаем необходимым: а) совершенствовать уголовное законодательство в русле уточнения категориально-понятийного аппарата, используемого при квалификации компьютерных мошенничеств, предусмотрения соизмеримой характеру и степени общественной опасности уголовной ответственности за совершение компьютерных мошенничеств на систематической основе; б) модернизировать работу правоохранительных органов, осуществляющих борьбу с компьютерным мошенничеством; в) усилить техническую защиту систем хранения безналичных денежных средств на банковских счетах; г) повысить общий уровень цифровой грамотности населения.

*Ключевые слова:* компьютерное мошенничество, профессиональный преступник, уголовный закон, кардеры, фишеры, криминальный профессионализм, киберпреступники

*Для цитирования:* Пивнева Л. В. Профессиональное компьютерное мошенничество как разновидность профессиональной преступной деятельности в современных условиях развития информационного пространства // Вестник Волгоградской академии МВД России. 2025. № 1 (72). С. 41—47.

# PROFESSIONAL COMPUTER FRAUD AS A TYPE OF PROFESSIONAL CRIMINAL ACTIVITY IN THE CURRENT CONDITIONS OF INFORMATION SPACE DEVELOPING

***Lyudmila Valeriyevna Pivneva***
Southwest State University, Kursk, Russia
Putilin Belgorod Law Institute of Ministry of the Interior of Russia, Belgorod, Russia, iPVmila@yandex.ru

*Abstract.* Currently, by using new information technologies, it is possible to quickly and conveniently perform various financial transactions in cashless form, and therefore large cash flows have moved into the virtual environment. However, these manipulations with financial resources still do not have a high degree of legal, organizational and technical protection. Consequently, not only ordinary citizens are actively exploring the information

space every year, but also professional criminals, whose activity is precisely focused on continuous gaining profit from committing crimes. As a result, the issues of criminological assessing activities of certain categories of criminals-professionals working in the virtual sphere are becoming particularly relevant.

Based on mentioned above, the purpose of the study is to determine the features of professional criminal activity of computer fraudsters in the context of the information space developing.

The article considers the main specializations of modern computer fraudsters (phishers and carders), identifies their inherent signs of criminal professionalism. It is established that they are becoming more professional every day. To counteract this criminal activity, we consider it necessary to: a) improve criminal legislation in sphere of clarifying the categorical and conceptual framework used while qualifying computer fraud; providing for criminal liability commensurate with the nature and degree of public danger for committing computer fraud on a systematic basis; b) modernize the work of law enforcement agencies engaged in combating computer fraud; c) strengthen the technical protection of cashless financial storage systems on bank accounts; d) increase the general level of public digital literacy.

*Keywords:* computer fraud, professional criminal, criminal law, carders, phishers, criminal professionalism, cybercriminals

*For citation:* Pivneva L. V. Professional computer fraud as a type of professional criminal activity in the current conditions of information space developing. Journal of the Volgograd Academy of the Ministry of the Interior of Russia, 41—47, 2025. (In Russ.).

Профессиональная преступность считается крайне опасным антиобщественным явлением, поскольку от уровня ее развития прямо зависит благосостояние и спокойствие общества и государства. Однако появляется достаточно много новых разновидностей профессиональной преступной деятельности, и связано это во многом с усложнением социально-экономических отношений в современном российском обществе, а главное — активной цифровизацией отечественной экономики. На данный момент информационно-телекоммуникационная сфера развивается достаточно интенсивно, и эту область активно осваивают не только обычные граждане, но и преступники, причем не только «рядовые», но и профессиональные [1]. И особое место в структуре киберпреступности имеет достаточно распространенное в последнее время компьютерное мошенничество [2], представляющее реальную опасность для современных финансовых операций, совершаемых в дистанционной форме [3].

Цель настоящей статьи — определить особенности профессиональной преступной деятельности компьютерных мошенников в современных условиях развития информационного пространства.

Основываясь на анализе современной специальной научной литературы и правоприменительной практики, под компьютерным мошенничеством следует подразумевать совокупность корыстно совершенных преступлений, в процессе выполнения которых лицом для достижения преступной цели (завладения чужим имуществом или правом на чужое имущество) [4] осуществляются различные манипуляции с данными, программами, аппаратной частью ЭВМ и т. п. [5] Стоит также отметить, что компьютерное мошенничество в первую очередь связано с противоправным умышленным искажением, изменением или раскрытием указанных данных [6] в целях получения материальной выгоды с помощью компьютерной системы, особенно с использованием коммуникационных, технологических возможностей сети Интернет [7]. Однако полагаем, что использование самого понятия «мошенничество» по отношению к такого рода преступлениям достаточно условно, поскольку данная разновидность общественно опасной деятельности предполагает передачу имущества либо права на имущество без непосредственного участия жертвы преступления, которая даже не догадывается о том, что тем или иным своим действием подтверждает право передачи преступнику денежных средств, иных материальных ценностей. В связи с этим такой волевой признак, как добровольность, свойственный обману (злоупотреблению доверием), в определенной степени (применительно к данной разновидности преступной деятельности) отсутствует. Хотя в специальной научной литературе при характеристике таких деяний используются именно указанные понятия.

Отдельно отметим, что компьютерное мошенничество меняется в настоящее время не только количественно, но и качественно, в первую очередь активно профессионализируясь, поскольку Интернет в настоящее время создает наиболее благоприятные условия для занятия этой разновидностью преступной деятельности. Как справедливо отмечает исследователь А. А. Комаров,

сегодня интенсивная коммерциализация сервисов в Интернете, а также появление новых финансовых услуг и инструментов сделали более прибыльным и безопасным осуществление привычных мошеннических схем в Сети. В результате традиционные мошеннические схемы быстро «перекочевали» в Интернет. Именно поэтому компьютерное мошенничество фактически стало исключительно профессиональным преступлением [1].

Общеизвестно, что в настоящее время профессиональные мошенники изобретают все более изощренные схемы обмана пользователей виртуальной сети, в результате чего жертва отдает преступникам крупные суммы денежных средств, иные материальные ценности. Компьютерные мошенники создают различные сайты-двойники, пользуются массовыми рассылками, а также персональными данными лиц, полученными в сети Интернет, для хищения финансов с банковских счетов и др.

Кроме того, сами технологии совершения компьютерного мошенничества заметно эволюционируют ввиду модернизации современных компьютерных систем, в первую очередь с технической точки зрения, причем занимаются этим нередко сами преступники. Указанные действия отдаленно напоминают схему создания вирусов и антивирусных программ, ведь как только сотрудники сферы информационной безопасности совершенствуют охранные системы в целях противодействия деятельности злоумышленников, преступники в свою очередь придумывают новые обходные пути, схемы обмана и т. п. Этот процесс непрерывен, в связи с чем данную разновидность преступной деятельности можно по праву считать сверхинтеллектуальной и особо профессионализованной сферой в условиях современности [8].

Примечательно, что среди компьютерных мошенников современные исследователи также выделяют такую группу преступников, как «профессионалы». Например, ученый В. Б. Верхов условно разделяет компьютерных мошенников на следующие три категории правонарушителей: лиц, отличающихся профессионализмом в данной сфере и определенным фанатизмом по отношению к своей деятельности; лиц, имеющих психические отклонения, в том числе страдающих «информационными» болезнями; профессиональных мошенников, «промышляющих» в сети Интернет с явно выраженными корыстными интересами. Вместе с тем, как подчеркивает исследователь, именно последняя группа преступников считается наиболее опасной для государства и общества, поскольку такие лица совершают практически 80 % преступлений, связанных с мошенничеством в виртуальном пространстве, причем в крупных и особо крупных размерах [9].

В свою очередь профессиональных компьютерных мошенников также подразделяют на группы в зависимости от их криминальной специализации. Так, некоторые исследователи выделяют среди таких «профессионалов» фишеров и кардеров [10].

Кардеры (от англ. card — кредитная карточка) — это лица, незаконно использующие информацию о платежных средствах, принадлежащую третьим лицам. Само понятие «кардерство» как вид мошенничества появилось недавно. Как отмечают ученые, способы хищения денежных средств с банковских карт, представляющих собой именные платежные документы, существенно отличаются от иных форм хищений [11]. Кроме того, современные исследователи выделяют среди этих преступников интернет-кардеров, или сетевых кардеров, работающих только с информацией, и реальных кардеров, которые совершают преступления с помощью пластиковых клонов кредитных карт [12].

Фишеры (от англ. fishing — рыбная ловля) — преступники, осуществляющие путем обмана пользователей сбор конфиденциальных данных о различных платежных средствах в своих корыстных целях [13]. Профессиональные фишеры, помимо обладания особыми техническими знаниями, умениями и навыками, владеют еще и методами и приемами социальной инженерии, позволяющими воздействовать, в том числе удаленно, на сознание человека. Занятие фишингом основано в первую очередь на незнании пользователей виртуальной сети норм сетевой безопасности [14]. Как правило, жертвами фишинга становятся клиенты банков, а также пользователи различных электронных платежных систем, посетители виртуальных аукционов, поскольку через получение доступа к учетным записям от тех или иных сервисов, к которым привязаны денежные средства, мошенники, как правило, и овладевают этими денежными средствами [15]. Особо примечательно, что наиболее изощренные способы совершения мошенничества, в частности фишинг, в настоящее время не нашли должного отражения даже в международном законодательстве [16].

Кроме того, у современных кибермошенников существуют не только «свои» специализации, но и хорошо отработанные схемы обмана, что также указывает на профессиональный характер деятельности преступников, их высокую криминальную квалификацию [17]. Так, в настоящее время

достаточно распространены различные махинации с криптовалютами. Профессиональные мошенники изобретают чуть ли не ежедневно новые способы получения материальной выгоды с помощью современных компьютерных систем. Например, в некоторой степени ноу-хау считается заражение программного обеспечения пользователя так называемым вирусом-вымогателем, который способен уничтожить все хранившиеся на компьютере данные и буквально парализовать работу всего программного обеспечения. Однако при этом «вирус-вымогатель» предлагает своей жертве пойти на своего рода сделку и за определенную плату вернуть утраченную информацию. Но даже после получения вирусом, т. е. преступником, создавшим и (или) запустившим этот вирус, денежных средств данные на компьютере, как правило, так и остаются в зашифрованном виде. И жертва не получает взамен ничего[1].

Отметим также, что в сообществе компьютерных мошенников за непродолжительный период их активной деятельности даже сложилась своя особая криминальная субкультура [10], поскольку их промыслу присуща устойчивость взглядов и выработанность особых норм поведения в виртуальном пространстве, что тоже указывает на профессиональный характер их деятельности. Форумы профессиональных компьютерных мошенников, иные площадки, на которых общаются, делятся опытом «профессионалы», в настоящее время имеют закрытый характер, за счет чего преступники обеспечивают себе неуязвимость от уголовного преследования [18]. Об этом говорит также высокая латентность указанного вида преступлений, которая, по отдельным данным, достигает в ряде случаев 95 % [19]. Вследствие этого неуязвимость от уголовного преследования, наряду с формированием внутри данного преступного сообщества собственной криминальной субкультуры, считаем необходимым отнести к признакам криминального профессионализма, позволяющим идентифицировать деятельность многих современных компьютерных мошенников как деятельность преступников-профессионалов.

Так, современным профессиональным компьютерным мошенникам свойственны такие признаки криминального профессионализма, как восприятие преступной деятельности в качестве средства для извлечения дохода, наличие криминальной субкультуры, преступной специализации и квалификации, «неуязвимость» от уголовного преследования. Все это в совокупности обязывает современных законодателей, правоприменителей, прочие заинтересованные субъекты, а также правоохранительные органы постоянно совершенствовать работу по противодействию промыслу профессиональных компьютерных мошенников [20], на что указывают и сами сотрудники МВД России[2]. Следовательно, можно заключить, что проблема борьбы с этой опасной разновидностью преступной деятельности давно стала серьезной для общества и государства в целом и для правоохранительных органов в частности.

Таким образом, в связи с широкой распространенностью, высоким уровнем латентности и значительной динамикой компьютерного мошенничества, его высокой степенью профессионализации считаем стратегической задачей современной политики российского государства решение данной проблемы. Для эффективного противодействия развитию этой разновидности преступной деятельности, учитывая существующие трудности в процессе защиты общественных отношений от посягательств компьютерных мошенников, находим целесообразным предпринять ряд мер. Важно и далее совершенствовать отечественное уголовное законодательство посредством уточнения категориально-понятийного аппарата, используемого при квалификации компьютерных мошенничеств, предусмотрения соизмеримой характеру и степени общественной опасности уголовной ответственности за совершение компьютерных мошенничеств на систематической основе. Кроме того, необходимо совершенствовать деятельность правоохранительных органов, осуществляющих борьбу с компьютерным мошенничеством, совершаемым в том числе на профессиональной основе, посредством внедрения в работу правоохранителей новых информационных технологий, общего повышения квалификации сотрудников в цифровых областях знаний, модернизации технических средств обнаружения и расследования компьютерных преступлений и обеспечения ими тех, кто занимается расследованием таких общественно опасных деяний. И, наконец, требуется усиление техниче-

[1] Десять схем кибермошенничества, о которых следует знать. URL: https://club.dns-shop.ru/blog/t-57-tehnologii/20007-desyat-shem-kiber-moshennichestva-o-kotoryih-vam-sleduet-znat/ (дата обращения: 02.06.2024).

[2] Международная конференция AntiFraud Russia — 2013 успешно завершила свою работу. URL: http://npc.ru/ru/media/news/?id=931 (дата обращения: 01.09.2024).

ской защиты систем хранения безналичных денежных средств на банковских счетах физических и юридических лиц, а равно и повышение общего уровня цифровой грамотности населения для противодействия профессиональным компьютерным мошенникам.

1. Комаров А. А. Компьютерное мошенничество в России и США: анализ количественных показателей за 2002—2012 гг. // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 172—177.

2. Бадзгарадзе Г. Д. О характеристике личности субъекта мошенничества в сфере компьютерной информации // КриминалистЪ. 2022. № 4 (41). С. 56—63.

3. Магомедов Г. М. К вопросу об использовании специальных знаний при расследовании мошенничеств, совершаемых при помощи электронных средств платежа // Закон и право. 2024. № 4. С. 209—212.

4. Самиулина Я. В. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации // Вестник Самарского юридического института. 2023. № 3 (54). С. 62—65.

5. Хайбрахманова А. Д. Вопросы квалификации мошенничества в сфере компьютерной информации: теория и практика // Юридическая наука. 2023. № 7. С. 267—276.

6. Семенихина Т. Н. О некоторых особенностях использования специальных знаний при расследовании дистанционных мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Общество и право. 2022. № 2 (80). С. 92—96.

7. Барокко Л. А. К вопросу об особенностях мошенничества, совершенного с использованием информационно-телекоммуникационных технологий по уголовному законодательству Российской Федерации // Вестник экономической безопасности. 2024. № 1. С. 15—19.

8. Коликов Н. Л. Профессиональная компьютерная преступность и мошенничество // Вестник ЮУрГУ. Серия «Право». 2011. № 40 (257). С. 61—64.

9. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. Москва: Горячая линия — Телеком, 2002. 336 с.

10. Гайфутдинов Р. Р. Типы компьютерных мошенников // Вестник экономики, права и социологии. 2017. № 2. С. 54—58.

11. Хисамова З. И. Кардерство в современной России // Вестник Краснодарского университета МВД России. 2012. № 3 (17). С. 97—100.

1. Komarov A. A. Computer-related fraud in Russia and the USA: quantity data analysis for the period of 2002—2012. Legal science and law enforcement practice, 172—177, 2016. (In Russ.).

2. Badzgaradze G. D. To the question of personality profile subjected to computer-related fraud. Criminalist, 56—63, 2022. (In Russ.).

3. Magomedov G. M. To the question of special knowledge application while investigating electronic payment fraud. Law and legality, 209—212, 2024. (In Russ.).

4. Samiulina Ya. V. Computer-related fraud: statutory regulation issues. Journal of the Samara Law Institute, 62—65, 2023. (In Russ.).

5. Khaibrakhmanova A. D. Computer-related fraud identification matters: theory and practice. Legal science, 267—276, 2023. (In Russ.).

6. Semenikhina T. N. Some peculiarities of special knowledge use while investigating computer-related remote transaction fraud. Society and law, 92—96, 2022. (In Russ.).

7. Barokko L. A. To the question of computer-related fraud peculiarities in the Russian Federation criminal legislature. Economic security journal, 15—19, 2024. (In Russ.).

8. Kolikov N. L. Professional computer crime and fraud. Journal of South Ural State University. "Law" series, 61—64, 2011. (In Russ.).

9. Kozlov V. Ye. Theory and practice of combating computer crime. Moscow; 2002: 336. (In Russ.).

10. Gayfutdinov R. R. Types of computer fraudsters. Economics, law and sociology journal, 54—58, 2017. (In Russ.).

11. Khisamova Z. I. Card fraud in contemporary Russia. Bulletin of Krasnodar University of Russian MIA, 97—100, 2012. (In Russ.).

12. Akindeeva A. V. Bank card fraud. Scientific letters of the St.-Petersburg branch named after Vladimir Bobkov of Russian Customs Academy, 263—271, 2005. (In Russ.).

13. Zavyalov A. N. Internet fraud (phishing): combat and prevention issues. Baikal research journal, 36—42, 2022. (In Russ.).

14. Pekareva V. V., Frolovskaya Yu. I. Researching the phishing phenomenon as a current issue of information space. Agricultural and land law, 101—102, 2023. (In Russ.).

12. Акиндеева А. В. Кардинг в сфере оборота банковских карт // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. 2005. № 2 (24). С. 263—271.

13. Завьялов А. Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. № 2. С. 36—42.

14. Пекарева В. В., Фроловская Ю. И. Исследование феномена фишинга как насущной проблемы информационного пространства // Аграрное и земельное право. 2023. № 10 (226). С. 101—102.

15. Жиделев В. Г. Некоторые аспекты квалификации преступлений в сфере компьютерной информации в российском и зарубежном законодательстве // Человек: преступление и наказание. 2012. № 2. С. 23—25.

16. Данько О. С., Медведева Т. А. Исследование техник фишинга и методов защиты от него // Молодой исследователь Дона. 2021. № 3 (30). С. 60—66.

17. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 135—141.

18. Полстовалов О. В., Галяутдинов Р. Р. Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения // Юридические исследования. 2023. № 11. С. 120—127.

19. Ершова Е. А. Некоторые вопросы «компьютерного мошенничества» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2009. № 1 (10). С. 103—107.

20. Филимонов С. А. Некоторые особенности борьбы с транснациональным компьютерным мошенничеством // Вопросы управления. 2014. № 5 (11). С. 236—243.

15. Dzydelev V. G. Some aspects of computer-related crime identification in Russian and international legislature. A person: crime and punishment, 23—25, 2012. (In Russ.).

16. Danko O. S., Medvedeva T. A. Researching phishing techniques and methods of protection against it. Young researcher of the Don, 60—66, 2021. (In Russ.).

17. Mogunova M. M. Implementation technology and the legal regulation of personal bank details theft (phishing). Journal of Saratov State Law Academy, 135—141, 2020. (In Russ.).

18. Polstovalov O. V., Galyautdinov R. R. Organised forms of online fraud: types of computer-related and high-tech fraud and peculiarities of their committing. Legal studies, 120—127, 2023. (In Russ.).

19. Yershova Ye. A. Some "computer-related fraud" issues. Legal science and practice: journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 103—107, 2009. (In Russ.).

20. Filimonov S. A. Some peculiarities of combating transnational computer-related fraud. Management issues, 236—243, 2014. (In Russ.).

***Пивнева Людмила Валерьевна*,**
аспирант кафедры уголовного права
Юго-Западного государственного
университета,
преподаватель кафедры
оперативно-разыскной деятельности
Белгородского юридического института
МВД России имени И. Д. Путилина;
iPVmila@yandex.ru

***Pivneva Lyudmila Valeriyevna,***
postgraduate student at the department
of criminal law
of the Southwest State University,
lecturer at the department of detective activities
of the Putilin Belgorod Law Institute
of Ministry of the Interior of Russia;
iPVmila@yandex.ru

Статья поступила в редакцию 10.01.2025; одобрена после рецензирования 20.01.2025; принята к публикации 14.02.2025.

The article was submitted 10.01.2025; approved after reviewing 20.01.2025; accepted for publication 14.02.2025.

* * *