УДК 34

Криминологические особенности организованного мошенничества в сфере информационных технологий

Красев Денис Валерьевич

Аспирант,
кафедра уголовного права и процесса,
Юридический институт,
190121, Российская Федерация, Санкт-Петербург, ул. Садовая, 21;
e-mail: denis.krasev@gmail.com

Аннотация

В статье рассматриваются актуальные криминологические аспекты организованного мошенничества в сфере информационных технологий. Автор анализирует современные тенденции развития кибермошенничества, выделяя характерные особенности данного вида преступной деятельности. Особое внимание уделяется эволюции методов совершения преступлений в цифровой среде и появлению новых инструментов противоправной деятельности. Исследование охватывает проблемы уголовной ответственности за преступления в сфере компьютерной информации, выявляет существенные пробелы в правовом регулировании и предлагает пути их устранения. Важное место в работе занимает анализ личности киберпреступника, исследование его мотивации и факторов, способствующих совершению преступлений в цифровой среде. Полученные результаты позволяют разработать эффективные меры профилактики и противодействия организованному кибермошенничеству, а также предложить рекомендации по совершенствованию законодательной базы.

Для цитирования в научных исследованиях

Красев Д.В. Криминологические особенности организованного мошенничества в сфере информационных технологий // Вопросы российского и международного права. 2025. Том 15. № 3А. С. 568-575.

Ключевые слова

Мошенничество, кибермошенничество, организованная преступность, информационные технологии, киберпреступность, личность преступника, уголовная ответственность, профилактика преступлений.

Введение

В ч. 2 ст. 23 Конституции Российской Федерации указано, что каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ограничение этого права допускается только на основании судебного решения [Конституция Российской Федерации, www]. Таким образом, тайна сообщений человека и гражданина подлежит повышенной защите.

Современное общество по всему миру, а также современное российское общество характеризуется постоянным развитием информационных технологий, однако, вместе с ростом популярности цифровых технологий, возрастает и уровень мошенничества в данной сфере. Сотни тысяч людей ежедневно становятся жертвами киберпреступников, в связи с чем, в уголовное законодательство были введены нормы, предусматривающие ответственность за такие преступления.

Согласно информации МВД РФ в январе-декабре 2022 года зарегистрировано 522,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [Краткая характеристика состояния преступности... 2022, www]. Однако, из-за сложности выявления и расследования таких преступлений, киберпреступники часто остаются безнаказанными.

Основное содержание

В контексте ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ [Уголовный кодекс Российской Федерации, www] приобретение права на чужое имущество является следствием мошеннических действий именно в компьютерно-информационной среде, когда происходит ввод информации, способствующей хищению, возникновению права на имущество, иные активы, удаления информации с целью совершения хищения, ее блокирования с целью недопущения доступа к информации, либо ее модификации, ведущей к искажению информации, вследствие чего возникают условия для совершения мошенничества [Мнацаканян, 2015, с.162].

В п. 20 постановления Пленума Верховного Суда Российской Федерации № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. разъясняется, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ.

Таким образом, документ судебного толкования также рекомендует в соответствующих случаях обращаться к совокупности преступлений [Постановление Пленума Верховного Суда РФ №48, www]. В соответствии с пунктом 21 данного постановления - хищение, осуществляемое посредством использования учетных данных владельца имущества, независимо от способа получения доступа к этим данным (тайно или обманным путем), квалифицируется как кража, если виновное лицо не оказывало незаконного воздействия на программное обеспечение серверов, компьютеров или информационно-телекоммуникационные сети.

Изменение данных банковского счета или движения денежных средств, произошедшее в результате использования учетных данных потерпевшего, не может быть квалифицировано по

статье 159.6 УК РФ («Мошенничество в сфере компьютерной информации»). В таких случаях, по нашему мнению, следует руководствоваться статьей 159 УК РФ («Мошенничество»).

Согласно анализу статей 273 («Создание, использование и распространение вредоносных компьютерных программ») и 159.6 УК РФ можно сделать вывод о том, что мошенническое программное обеспечение (мошеннические программы) по своему воздействию на компьютерную информацию аналогично вредоносным компьютерным программам.

В качестве примеров мошеннических программ можно привести: баннеры, блокирующие доступ к Интернету, программы-шифровальщики и др. Отметим, что для устранения негативных последствий действия таких программ от потерпевшего часто требуется отправка платного СМС сообщения на указанный номер.

Таким образом, считаем, что необходим дифференцированный подход к квалификации мошеннических действий в зависимости от используемых методов и целей.

Динамичное развитие электронных систем и коммуникаций и их повсеместное внедрение способствовало увеличению количества совершаемых в соответствующих сферах преступлений. При этом большая часть посягательств происходит в сфере дистанционного банковского обслуживания и электронной коммерции, что напрямую влияет на устойчивость экономики государства [Хисамова, 2015, с. 128].

Безналичная система расчетов на основе использования банковских платежных карт продолжает активно внедряться в кредитно-финансовую сферу деятельности нашей страны, являясь при этом привлекательным объектом, как для отдельных преступников, так и для организованных преступных групп. Расширение спектра предоставленных банками услуг в безналичной сфере расчетов неизбежно приводит к изменениям в структуре экономической преступности [Хисамова, 2012, с. 97].

Рассуждая о мошенничестве в сфере цифровой информации, нельзя не сказать о мошенническом программном обеспечении, позволяющем нарушать системы защиты цифровой информации. Сегодня зачастую такое программное обеспечение находится в свободном доступе в сети Интернет или же нелегально приобретается на соответствующих виртуальных площадках у их разработчиков. Таким образом, ограничение в создании, использовании и распространении такого программного обеспечения существенно затруднило бы злоумышленникам совершение подобного рода мошенничеств. Это также касается рассматриваемых программ и программных средств, используемых для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей [Бегишев, 2016, с. 28].

Более глубокое изучение личности преступника как одного из центральных факторов механизма совершения преступления даёт возможность сформировать полное представление о мотивах преступной деятельности. На основе этого понимания можно разработать наиболее эффективные меры по предотвращению преступлений.

Проведенный анализ научной литературы позволяет прийти к выводу о том, что в структуре личности преступника традиционно принято выделять три подсистемы: социально-демографические признаки, социальные функции личности, а также нравственно-психологические характеристики [Шестаков, 2019, с. 42].

Указанные структурные признаки в совокупности формируют целостный комплекс взаимозависимых элементов, составляющих личность преступника и определяющих ее криминологическую природу.

Для более детального изучения криминологической характеристики личности мошенника,

использующего телекоммуникационные и компьютерные сети, необходимо провести непосредственный анализ.

Социально-демографическая характеристика личности такого мошенника основывается на таких параметрах, как: пол, возраст, социальный статус и прочие факторы.

Как справедливо отмечает, Р. И. Дремлюга, «комплекс элементов, раскрывающих социально-демографическую характеристику личности мошенников, позволяют выявить наличие определенных отклонений в системе социализации мошенников и служат информационной основой для общесоциальной и специально-криминологической профилактики хищений» [Дремлюга, 2008, с. 63].

Интернет-мошенники делятся на две большие группы:

Во-первых, лица, которые находятся с потерпевшим в деловых или трудовых отношениях;

Во-вторых, лица, которые не имеют деловых отношений с потерпевшим [Русаков, 2015, с. 207].

Первая категория включает сотрудников, злоупотребляющих своим служебным положением для получения незаконной выгоды. К ним относятся: представители технического персонала, сотрудники служб безопасности и надзора, а также лица, принимающие решения по организационным вопросам.

Вторая категория охватывает лиц, обладающих глубокими знаниями в области интернет-технологий и руководствующихся преимущественно корыстными мотивами. В эту группу входят, как профессиональные специалисты (хакеры), воспринимающие меры безопасности компьютерных систем как вызов своему профессионализму, так и лица, использующие в своей деятельности мошеннические схемы.

Анализ осужденных по статьям 159.3 и 159.6 Уголовного Кодекса Российской Федерации показывает, что данная категория преступников, как правило, обладает средним профессиональным образованием и достигла возраста старше 30 лет. Это связано с тем, что совершение мошенничества в сфере цифровых технологий требует высокого уровня интеллекта, технической грамотности, а также глубоких знаний в области информационных технологий, программирования и компьютерных сетей.

Динамика преступлений, совершаемых лицами в возрасте от 18 до 24 лет, обусловлена, в частности, процессом социализации и вступления в самостоятельную жизнь. К этой категории относятся: выпускники школ, студенты вузов и колледжей, а также лица, не продолжившие обучение после окончания средней школы.

Важно отметить, что у данной возрастной группы наблюдается низкий уровень ответственности перед обществом. В связи с этим, преступность и криминальная субкультура воспринимаются ими как нечто «романтическое». Кроме того, вследствие минимального уровня личных доходов, они фактически и психологически зависят от заработной платы своих родителей (законных представителей).

Соответственно, все это приводит к тому, что представители данной возрастной группы довольно часто находятся в состоянии психологического дискомфорта, обусловленного не только сравнением себя с более обеспеченными сверстниками, но и фактическим отсутствием возможности повысить свой социальный статус посредством увеличения доходов законным путем.

Большинство подростков активно используют развлекательные ресурсы (социальные сети и др.), что приводит к снижению уровня их технических знаний, умений и навыков. В результате современная молодежь в большей степени не обладает необходимыми компетенциями, которые

могли бы быть использованы для совершения преступлений в сфере цифровых технологий.

Как справедливо отмечает, Д. О. Теплова «отсутствие роста доли несовершеннолетних объясняется также сложностью мошеннического способа хищения, кроме того, при определенных способах совершения преступления злоумышленник может достигнуть «успеха» лишь при наличии определенного доверия к нему со стороны потерпевшего. Подростку труднее завоевать такое доверие, когда речь идет об имущественных интересах» [Теплова, 2014, с. 248].

При анализе уровня образования указанной категории преступников следует подчеркнуть наличие у них высоких технических навыков, что значительно облегчает им совершение преступлений и сокрытие следов преступления.

Помимо высокого уровня образования и технической компетентности, данная категория преступников демонстрирует стремление к самосовершенствованию. Это способствует выявлению ими уязвимостей и недостатков в существующих системах (как компьютерных, так и социальных), что создаёт условия для увеличения их противоправной выгоды.

В целом, проведенное исследование подтвердило известный криминологический тезис о том, что «образование и социальный статус преступника предопределяют сложность и изощренность преступного поведения» [Кудрявцев, Эминов, 2010, с. 71].

Использование компьютерной и мобильной техники стало привычным явлением. Поэтому важно отличать лиц, совершающих мошеннические действия с использованием телефонов, компьютеров и других информационно-телекоммуникационных технологий (традиционных интернет-мошенников) от профессиональных киберпреступников, применяющих передовые средства анонимизации в сети Интернет (VPN, TOR-браузер и др.), анонимные VoIP-звонки, с целью получения незаконной прибыли, в том числе в составе организованных групп.

Подавляющее большинство зарегистрированных случаев мошенничества, совершенных с использованием информационно-телекоммуникационных технологий, приходится на традиционные схемы.

Классические интернет-мошенники в ходе осуществления преступного замысла используют давно известные предлоги мошеннических действий, совершаемых посредством компьютерных технологий и средств мобильной связи: продажа (покупка) товаров посредством различных интернет-ресурсов (Авито, Юла и т. п.) в том числе «фишинговых», сообщение ложных сведений о выигрыше приза, ложная информация о задержании близких лиц за совершение различных правонарушений, компенсация за ранее приобретенные биологически-активные добавки (медицинские препараты, оборудование) и другие [Аксенов, Молчанова, 2020, с. 80].

Следовательно, тип мошенничества, на котором специализируется преступник, во многом определяется его индивидуальными характеристиками. Криминологический портрет типичного интернет-мошенника характеризуется следующими чертами:

– Пол: преимущественно мужской.
– Возраст: от 18 до 35 лет.
– Место жительства: город.
– Образование: среднее профессиональное или среднее.
– Принадлежность к субкультуре: активное участие в закрытых онлайн-форумах, знание специфической терминологии и жаргона.

Важно также отметить, что уровень квалификации преступников может варьироваться от высококвалифицированных специалистов до дилетантов.

Ключевой особенностью мошеннических действий в сфере цифровых технологий является использование интернета и социальных сетей для привлечения жертв. Преступники создают

поддельные профили и сайты, распространяют спам и фишинговые письма с целью получения доступа к персональным данным и финансовым ресурсам. Взлом аккаунтов и использование вредоносных программ также являются распространенными методами. Анонимность, предоставляемая интернетом, затрудняет идентификацию и привлечение к ответственности преступников.

Заключение

Таким образом, исходя из всего вышеизложенного, считаем, что для эффективной борьбы с интернет-мошенничеством необходимо применение строгих, но справедливых наказаний. Такое наказание должно иметь профилактическую функцию, обескураживание потенциальных преступников и предотвращение будущих преступлений.

Также мошенничества в сфере цифровых технологий характеризуются высокой степенью латентности и низким процентом раскрываемости. К основным причинам этого относятся: постоянная адаптация киберпреступников к новым методам защиты информации; анонимность, предоставляемая интернетом; недостаточная осведомленность пользователей о рисках и мерах защиты от интернет-мошенничества.

Следовательно, считаем, что противодействие интернет-мошенничеству является одной из важнейших задач для всех заинтересованных сторон: пользователей, организаций, государственных структур и международного сообщества. Только совместными усилиями можно разработать и реализовать эффективные меры предотвращения и борьбы с киберпреступностью.

Библиография

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // www.consultant.ru; Комментарий к Конституции Российской Федерации. 5-е изд., испр. и доп. // Под ред. проф. С.А. Комарова. – М.: Изд-во «Юрайт», 2023. – 325 с. (Серия: Профессиональный комментарий).
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 30.12.2023) // www.consultant.ru.
3. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // www.consultant.ru.
4. *Аксенов В. А., Молчанова Т. В.* Особенности личности современного интернет-мошенника в механизме индивидуального преступного поведения // Криминологический журнал, 2020. – № 4. – С. 79 - 86.
5. *Антонян Ю. М.* Личность преступника. Криминология: учебник / под ред. В. Н. Кудрявцева, В. Е. Эминова. – 4-е изд., перераб. и доп. – М.: Норма, 2009. – 368 с.
6. *Бегишев И. Р.* Новый взгляд на мошенничество в сфере компьютерной информации // Information Security / Информационная безопасность. – 2016. – № 1. – С. 28 - 29.
7. *Долгова А. И.* Криминология: учебник для вузов. – 4-е изд., перераб. и доп. (ГРИФ) / А. И. Долгова. – М.: ИНФРА-М, Норма, 2010. – 1008 с.
8. *Дремлюга Р. И.* Интернет-преступность. – Владивосток: изд-во Дальневосточного университета, 2008. – 238 с.
9. *Ким Е. В., Ри П. Г.* Личность преступника: криминологический анализ // Электронное научное издание «Ученые заметки ТОГУ», 2013. – Т. 4. – № 4. – С. 402-407.
10. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2022 года. Министерство внутренних дел РФ. ФКУ «Главный информационно-аналитический центр»
11. *Кудрявцев В. Н., Эминов В. Е.* Криминология: учебник / под ред. В. Н. Кудрявцева, В. Е. Эминова. – М.: Норма: Инфра, 2010. – 800 с.
12. *Мнацаканян А. В.* Информационная безопасность Российской Федерации: уголовно-правовые аспекты: дис. … канд. юрид. наук. – М., 2015. – 216 с.
13. Официальный сайт Судебного департамента при Верховном Суде РФ: URL: http://cdep.ru/.
14. *Познышев С. В.* Криминальная психология. Преступные типы. О психологическом исследовании личности как

субъекта поведения вообще и об изучении личности преступника в частности // Юридическая психология. – 2008. – № 2. – С. 8-13.
15. *Родимушкина О. В*. К вопросу о личности преступника – девианта, совершающего корыстно-насильственные преступления // Российский следователь. – 2009. – № 17. – С. 32-34.
16. *Русаков И.М.* Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Вестник Краснодарского университета МВД России. – 2015. – № 4. – С. 206-208.
17. *Теплова Д. О.* Криминологическая характеристика и предупреждение организованного мошенничества: дис…. канд. юрид. наук. — М., 2014. — с. 248.
18. *Хисамова З. И.* Кардерство в современной России // Вестник Краснодарского университета МВД России. 2012. № 3 (17). С. 97 - 100.
19. *Хисамова З. И.* Квалификация посягательств, совершенных с использованием электронных средств платежа // Государство и право. 2015. № 3. С. 127 - 132.
20. *Шестаков Д. А.* Криминология: учебник для вузов. — М.: «Юридический Центр Пресс», 2019. — 400 с.

Criminological Features of Organized Fraud in the Information Technology Sector

Denis V. Krasev

Postgraduate Student,
Department of Criminal Law and Procedure,
Law Institute,
190121, 21, Sadovaya str., Saint Petersburg, Russian Federation;
e-mail: denis.krasev@gmail.com

Abstract

The article examines current criminological aspects of organized fraud in the information technology sector. The author analyzes modern trends in the development of cyber fraud, identifying characteristic features of this type of criminal activity. Particular attention is paid to the evolution of methods for committing crimes in the digital environment and the emergence of new tools for unlawful activities. The study covers problems of criminal liability for computer-related crimes, reveals significant gaps in legal regulation, and proposes ways to address them. An important part of the work is devoted to analyzing the profile of cybercriminals, examining their motivations and factors contributing to the commission of crimes in the digital environment. The obtained results enable the development of effective measures for the prevention and counteraction of organized cyber fraud, as well as recommendations for improving the legislative framework.

For citation

Krasev D.V. (2025) Kriminologicheskie osobennosti organizovannogo moshennichestva v sfere informatsionnykh tekhnologiy [Criminological Features of Organized Fraud in the Information Technology Sector]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (3A), pp. 568-575.

Keywords

Fraud, cyber fraud, organized crime, information technology, cybercrime, criminal profile, criminal liability, crime prevention.

References

1. "The Constitution of the Russian Federation" (adopted by popular vote on 12/12/1993 with amendments approved during the nationwide vote on 07/01/2020) // www.consultant.ru ; Commentary to the Constitution of the Russian Federation. 5th ed., ispr. and add. // Edited by N. prof. N. St.A. N. Komarov. - M. N.: Publishing house "Yurayt", 2023. – 325 p. (Series: Professional Commentary).
2. "The Criminal Code of the Russian Federation " dated 13.06.1996 No. 63-FZ (as amended on 25.12.2023) (with amendments and additions, intro. effective from 12/30/2023) / / www.consultant.ru .
3. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 11/30/2017 No. 48 (as amended on 12/15/2022) "on judicial practice in cases of fraud, embezzlement and embezzlement" / / www.consultant.ru .
4. V. Aksenova, A. N., Molchanova, T. N., V. N. Personality features of a modern Internet fraudster in the mechanism of individual criminal behavior // Criminological Journal, 2020, No. 4, pp. 79-86.
5. Yu. Antonyana, M. N. The identity of the criminal. Criminology: textbook / Edited by N. V. N. N. Kudryavtsev, V. N. E. N. Eminov. - 4th ed., revised and add. - M. N.: Norma, 2009. - 368 p. ill.
6. I. Begisheva. PH. A new look at fraud in the field of computer information // Information Security / Information security. – 2016. – No. 1. - St. 28-29.
7. A. Dolgova. I. N. Criminology: textbook for universities. - 4th ed., revised and add. (VULTURE) / A. N. I. N. Dolgova. - M. N.: In-FRA-M, Norma, 2010. - 1008 p. ill.
8. R. Dremlyuga. I. N. Internet crime. Vladivostok: Publishing House of the Far Eastern University, 2008. 238 p. ill.
9. E. Kim. V. N., P. Ri. G. N. Criminal identity: criminological analysis // Electronic scientific publication "Scientific notes of TOGU", 2013. - D. N. 4. – No. 4. - St. 402 407.
10. Brief description of the state of crime in the Russian Federation for January-December 2022, Ministry of Internal Affairs of the Russian Federation. FKU"Main Information and Analytical Center"
11. V. Kudryavtseva, N. N. Eminov, V. N. E. N. Criminology: textbook / Edited by N. V. N. N. Kudryavtsev, V. N. E. N. Eminov. - M. N.: Norm: Infra, 2010. - 800 p. ill.
12. A. Mnatsakanyan. V. N. Information security of the Russian Federation: criminal law aspects: dissertation of the candidate. jurid. M. N., 2015, 216 p. ill.
13. Official website of the Judicial Department at the Supreme Court of the Russian Federation: URL: http://cdep.ru /.
14. S. Poznyshev, V. N. Criminal psychology. Criminal types On the psychological study of personality as a subject of behavior in general and on the study of the personality of a criminal in particular // Legal Psychology. - 2008. – No. 2. - St. 8-13.
15. O. Rodimushkina. V. N. On the question of the identity of a deviant criminal who commits mercenary and violent crimes // A Russian investigator. – 2009. – No. 17. - St. 32 34.
16. I. Rusakova, M. N. Criminalistic characteristics of the personality of a criminal who committed fraud in the provision of Internet services // Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. – 2015. – No. 4. - St. 206-208.
17. D. Teplova. According to O. N. Criminological characteristics and prevention of organized fraud: dis.... cand. jurid. Sciences. - M. N., 2014. - St. 248.
18. Z. Khisamova. I. N. Carding in modern Russia // Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2012. No. 3 (17). Articles 97-100.
19. Z. Khisamova, I. N. Qualification of encroachments committed using electronic means of payment // State and law. 2015. No. 3. Articles 127 - 132.
20. D. Shestakova. A. N. Criminology: textbook for universities. - M. N.:"Law Center Press", 2019. - 400 p. ill.