УДК 343.721

***А. Е. Крупская*[1], *Е. Р. Воробьева*[1]**
[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ОНЛАЙН-МОШЕННИЧЕСТВА

Аннотация. *В статье рассматриваются вопросы уголовно-правовой характеристики мошенничества в целом и онлайн-мошенничества в частности. Приводятся статистические данные, виды и схемы мошенничества, возможные наказания за подобные преступные действия. Предложены мероприятия по сокращению случаев мошенничества.*

Ключевые слова: *уголовное право; мошенничество; киберпреступность; обман; информационные данные.*

E. R. Vorobyova[1], A. E. Krupskaya[1]
[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

CRIMINAL LAW CHARACTERISTICS OF ONLINE FRAUD

Abstract. *The article examines the criminal-legal characteristics of fraud in general and online fraud in particular. Provides statistical data, types and schemes of fraud, possible punishment for such criminal acts. Measures are proposed to reduce fraud.*

Keywords: *criminal law; fraud; cybercrime; deception; informational data.*

Познавая правовую действительность, следует четко различать эмпирические и теоретические формы научного юридического знания [1, с. 44]. Настоящая статья представляет собой эмпирический анализ практики применения уголовного закона о мошенничестве. В качестве исходной методологической посылки следует признать суждение о том, что применение принципов права является одним из инструментов преодоления дефектности норм законодательства [2, с. 28].

К мошенничеству относится хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Любое мошенничество является преступлением, за которое придется отвечать согласно статьям 159–159.6 Уголовного кодекса Российской Федерации [3]. В целях обеспечения единообразного применения судами норм уголовного закона об ответственности за мошенничество Пленум Верховного Суда Российской Федерации сделал соответствующие разъяснения [4].

Принципиальным отличием мошенничества от кражи является то, что жертву обманывают и она по собственной воле отдает свое имущество или права на его использование. В юридической литературе соответствующие вопросы уголовно-правовой характеристики данной категории преступлений получил детальное освящение [5, с. 13–15], [6, с. 45–48], [7, с. 17–21]. К сожалению, мошенничество всегда являлось и является по сей день наиболее сложно раскрываемым преступлением, к тому же с каждым годом у мошенников появляются новые области применения своих преступных возможностей (такие как интернет, социальные сети и мобильная связь).

Так как виртуальная «жизнь» людей совсем молода, она не подчиняется устоявшимся общепризнанным законам и правилам. Основной проблемой раскрытия преступлений подобного рода является то, что взаимоотношения жертвы и преступника происходят таким образом, что преступник сохраняет статус «инкогнито», что дает соблазн действовать по отношению к нему незаконно и неограниченное количество раз. В настоящее время сеть интернета стала очень популярной: каждый день ей пользуется более трех миллиардов человек в мире, а мобильной связью пользуется еще активнее. Неудивительно, что мошенники выбирают именно это поле деятельности.

Число афер в сети или с использование мобильной связи увеличивается вместе с количеством пользователей каждый день. Согласно статистическим данным, за 10 месяцев в 2016 г. на территории Северо-Западного административного округа города Москвы зафиксировано 1 111 афер общеуголовной ориентированности из них свыше 600 посредством мо-

бильной связи либо сеть интернет. На первый взгляд, может показаться, что в ряды жертв чаще всего попадают старики, инвалиды и подростки, но по статистике на данные категории лиц приходится лишь 18 процентов потерпевших, оставшиеся 82 процента – это молодые люди и лица среднего возраста.

Онлайн-мошенничество возглавляет список менее раскрываемых преступлений, но правоохранительные органы не бездействуют и прилагают всевозможные усилия для раскрытия таких сложных мошеннических схем. Так например, за десять месяцев этого года, по сравнению с аналогичным периодом 2015 г. раскрыто на 24 процента больше преступлений. Чаще всего онлайн-мошенничества имеют серийный характер, поэтому раскрытие одного преступления влечет за собой раскрытие еще нескольких.

Термин «онлайн» определяется как «управляемый», «подключён к компьютеру» или как «деятельность, которая доступна исключительно через Интернет». Отталкиваясь от представленных определений, определим что такое онлайн-мошенничество.

Онлайн-мошенничество – это действия киберпреступников, направленные на завладение информационными данными или финансовыми средствами пользователя интернета.

Основная цель у мошенников – обмануть и получить денежные средства либо иное имущество. При этом неважно в каком месте они будут это делать – на улице, в торговом центре либо на веб-сайтах и по электронной почте. В сети интернет можно отыскать жертву, не общаясь с ней вживую. Мошенники могут располагать к себе. Среди них есть эксперты по психологии, экономике, страхованию, финансам, а так же специалисты по многим другим областям.

На рисунке 1 приведена статистика по преступности по ст. 159–159.6 УК РФ за апрель-июнь 2019 и 2020 гг.

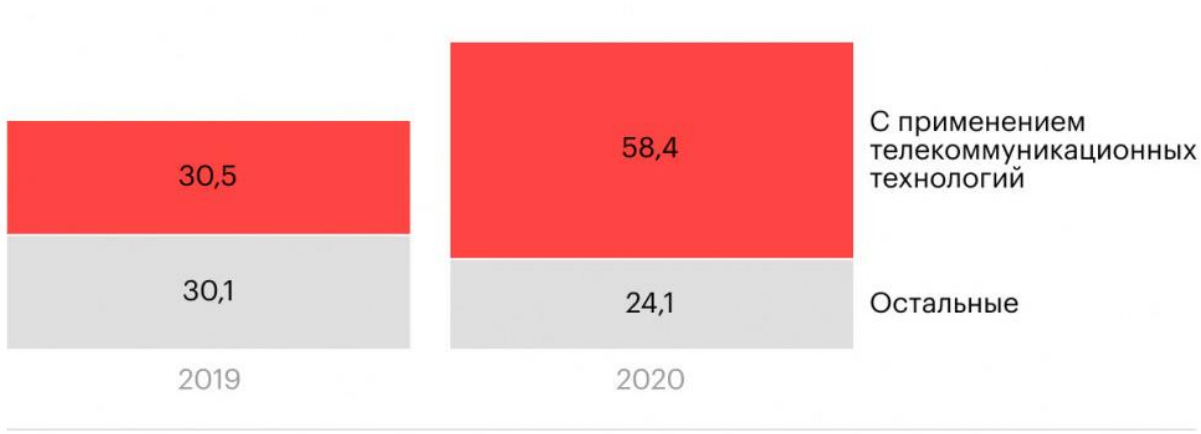

Рис. 1. Количество зарегистрированных преступлений по ст. 159–159.6 УК РФ за второй квартал 2019 и 2020 гг.

Из этих данных можно сделать вывод, что количество преступлений с использованием телекоммуникационных технологий:

1) возрастает с каждым годом, практически в два раза;

2) составляет половину преступлений от общего числа в 2019 г. и две трети от общего числа преступлений в 2020 г.

У мошенников есть специальные форумы, на которых можно приобрести все необходимое для «работы»: свежие схемы мошенничества, сим-карты и банковские карты, оформленные на подставных лиц, пароли и специальные программы для VPN-соединения, загрузочные флешки с операционными системами, которые не оставляют следов в интернете, и многое другое.

В наше время существует огромное количество мошеннических схем в интернете. Можно назвать самые распространенные.

Обман в интернет-банкинге – это обман либо хищение, совершенное с применением интернет-технологий, соответственно цель – незаконно увести средства либо переместить их на другой банковский счет. Совершение преступления также может производиться через телефон, планшет и прочие мобильные устройства. Мобильный банкинг в вашем компьютере, планшете либо телефоне на сегодняшний день весьма удобен и привычен каждому. Банки, в свою очередь, защищают ваши счета с помощью сложных программных систем. Правонарушители понимают, что подобные системы обходить очень трудно, по этой причине они фокусируются напрямую на клиентах, обманывая жертв и вынуждают их раскрыть конфиденциальные данные. В российском законодательстве не до конца выясненным является вопрос о квалификации хищения с банковской карты в свете Определения Верховного Суда РФ от 29 сентября 2020 г. [8]. Отсутствие единообразного подхода в практике судов с момента внесения изменений в ст. 158 УК РФ (введения признака кражи с банковского счета) создает правовую неопределенность при выборе применяемой нормы в случае оплаты товаров и услуг чужой банковской картой – как кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ) либо как мошенничества с использованием электронных средств платежа (ст. 159.3 УК). В юридической литературе обосновывается вывод о том, что хищение, совершенное путем использования чужой банковской карты при покупке товаров в торговой организации, должно квалифицироваться как мошенничество с использованием электронных средств платежа по ст. 159.3 УК РФ [9, с. 39]. В этой связи отдельные ученые справедливо обозначают вопросы, которые потребуется решить законодателю [10, с. 35–37].

Фишинг – это использование спама с целью того, чтобы мошенническим путем получить доступ к сведениям интернет-банкинга. Термин «фишинг» происходит от слова «to fish» – «ловить на удочку». Модель простая, используются спамовые электронные письма, якобы от банка. Подобным способом правонарушители «ловят рыбу» – информацию с целью входа в законный банковский счет клиента. Правонарушители направляют огромное число электронных писем на случайные адреса электронной почты в надежде завлечь ничего не подозревающих невинных людей, чтобы те предоставили собственные личные банковские реквизиты. Как правило, фишинговый адрес с электронной почты будет требовать клиента перейти по гиперссылке фальшивого банковского веб-сайта на страницу интернет банкинга также ввести личные банковские реквизиты. Зачастую перейдя по ссылке, жертва также скачивает вредоносные программы, что фиксирует нажатия кнопок на клавиатуре, включая различную введенную информацию, такую как данные банковского входа и посылает их третьей стороне.

Мошеннические схемы – это методы отъема средств с помощью обмана. Такие схемы существовали всегда и везде, однако ничего не стоит на месте и основной проблемой мошенников всегда был и останется постоянный обмен информацией, так как любой способ обмана, приносивший доход мошенникам, перестает работать, так как люди узнают как это работает и становятся бдительней. Поэтому мошенникам постоянно приходится придумывать новые схемы обмана.

Самыми распространенными схемами мошенничества в 2019–2020 гг. являются следующие схемы:

1. *Телефонное мошенничество* – звонит служба финансового контроля банка «N», а затем возможно несколько вариантов развития:

– вам говорят о том, что с вашей карты была попытка снятия 2 000 рублей и уточняют вы ли снимаете деньги; большинство людей впадают в панику, говорят, что деньги они с карты не снимают, тогда «банк» просит назвать номер вашей карты и код из трех цифр; испуганный клиент называет данные и мошенник получает доступ к вашим данным и переводит ваши средства на свой счет;

– вам говорят о том, что на вашу карту случайно зачислены средства неизвестным пользователем и для отмены перевода просят назвать данные карты;

– вам предлагают заняться инвестициями, отправляют ссылку, по которой вы переходите, и в это время мошенник перехватывает ваши данные.

2. *Обман фрилансеров*. Практически каждый фрилансер, особенно начинающий, сталкивался со случаем, когда он брался за работу без предоплаты, а после того как работа была выполнена заказчик пропадал. Большинство сразу понимает в чем дело и пересматривает условия своей работы.

3. *Лжеблаготворительность* – вам приходит сообщение, открывается реклама или на личной станице в социальной сети вы видите сообщение «Моя мама (дочь и т.д.) умирает!» После такого громкого заголовка идет душераздирающая история, в которой описано что и как произошло. Это всегда так трогательно, что руки сами тянутся к кошельку. Однако нужно сохранять здравый смысл и перед тем как совершать «благой» поступок проверить достоверность информации. Проверить фонд или позвонить друзьям, если подобное сообщение было опубликовано от их имени. Лжеблаготворительность является распространенным видом мошенничества и будет обидно, если вместо помощи нуждающимся ваши честно заработанные деньги уйдут очередному лжецу.

Рис. 2. Количество случаев мошенничества за 2016–2020 гг.

4. *Мошенники инфобизнеса*. Уже после того, как население стало больше верить интернет-курсам, в сети развелось большое количество ушлых инфобизнесменов, обещающих обучить чему угодно – от игры на скрипке и до прокачивания софт-скиллов. При этом сами они в этом могут не разбираться, однако их вряд ли это остановит, ведь как говорится «деньги не пахнут».

На рисунке 2 представлена информация о том как изменилось число случаев мошенничества за время самоизоляции.

Проведя анализ данных можно сделать следующие выводы:

1) общее число случаев мошенничества в 2020 г. увеличилось на 20 000 случаев и резко возросло; на протяжении четырех лет количество было примерно равным и представлялось неким плато;

2) мошенничество сократилось в отраслях компьютерной информации, сфере страхования, сфере кредитования и при получении выплат; скорее всего это связано с ужесточением контроля этих сфер, в компьютерной информации произошли большие открытия, вперед шагнула сама система информационной безопасности, сфера страхования ужесточила контроль и описание страховых случаев, во многих организациях появилось добровольное медицинское страхование (ДМС), а так же многие виды страхования стали обязательными при заключении договоров и сделок разных видов. Банки так же стали надежнее предоставлять кредиты и процедура их получения с каждым днем улучшается. Что касается материальных выплат, то, во-первых, их число увеличилось, а, во вторых, способ их получения стал безопаснее;

3) но есть одна группа мошенничества, которая обеспечивает значительный прирост числа данного вида преступлений – мошенничество с банковскими картами (ст. 159.3 УК РФ). Данная статья о мошенничестве с использованием электронных средств платежей была ужесточена и дополнена в мае 2018 г. Для сравнения: в 2016 г. было зарегистрировано 96 случаев таких преступлений, а на середину 2020 г. – 8 053 случаев. Страшно представить какое количество преступлений будет совершено к концу 2020 г. Конечно, изоляция и карантин заставили уходить в онлайн-бизнес, но системы платежей не были готовы к такому количеству атак, люди не были образованы в сфере обращения с электронными системами платежей и банковскими картами, что обмануть их было очень просто.

Чтобы уберечься от подобных «учителей», постоянно гуглите отзывы. Даже если человек по ту сторону экрана кажется вам харизматичным, компетентным и честным – вы можете заблуждаться.

В Российской Федерации наказание за мошенничество определено по статьям 159–159.6 УК РФ.

В период карантина онлайн-бизнес вырос в своих объемах и участились случаи онлайн-мошенничества, поэтому необходимо пересмотреть и ужесточить наказания, а также заняться обучением населения как не попасться на удочку мошенника. Создать доступные базы для проверки карт и номеров счета, запретить организациям передавать персональную информацию третьим лицам для рекламы. Логичным и обоснованным представляется закрепление на уровне Федеральных государственных образовательных стандартов высшего образования такой компетенции как финансовая грамотность [11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Пахаруков А.А. Структура научного знания: эмпирический и теоретический уровни (на примере юридической науки) // Культура. Наука. Образование. 2019. № 3. С. 23–57.

2. Пахаруков А.А. Реализация принципа соразмерности в правовом регулировании отношений несостоятельности // Приложение к журналу Предпринимательское право «Право и бизнес». 2018. № 3. С. 28–32.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

4. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2.

5. Григорян Г.Р. О социально-правовой сущности корыстных имущественных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Российская юстиция. 2020. № 10. С. 13–15.

6. Олейник Е.Н. Объект мошенничества с использованием электронных средств платежа // Уголовное судопроизводство. 2020. № 3. С. 45–48.

7. Макаров А.В., Шадрин Д.А. К вопросу о квалификации хищений с использованием информационно-телекоммуникационных технологий на объектах транспорта (по материалам Забайкальского ЛУ МВД России на транспорте) // Транспортное право. 2020. № 3. С. 17–21.

8. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6. Текст : электронный // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru (дата обращения: 28.11.2020).

9. Яни П.С. Хищение с использованием чужой банковской карты в магазине следует квалифицировать как мошенничество // Законность. 2020. № 12. С. 39–43.

10. Филатова М.А. Хищение с использованием чужой банковской карты в магазине образует состав кражи // Законность. 2020. № 12. С. 34–38.

11. Пахаруков А.А. Примерная основная образовательная программа высшего юридического образования как модель реализации компетентностного подхода: вопросы правового регулирования // Известия Байкальского государственного университета. 2016. Т. 26, № 1. С. 115–122.

REFERENCES

1. Pakharukov A.A. Struktura nauchnogo znaniya: empiricheskiy i teoreticheskiy urovni (na primere yuridicheskoy nauki) [Structure of Scientific Knowledge: Empirical and Theoretical Levels (On the Example of Legal Science]. *Kul'tura. Nauka. Obrazovaniye* [*Culture. Science. Education*], 2019, No. 3, pp. 23-57.

2. Pakharukov A.A. Realizatsiya printsipa sorazmernosti v pravovom regulirovanii otnosheniy nesostoyatel'nosti [Implementation of the Proportionality Principle in the Legal Regulation of Insolvency Relationships]. *Prilozheniye k zhurnalu Predprinimatel'skoye pravo «Pravo i biznes»* [*Appendix to the journal Entrepreneurial Law "Law and Business"*], 2018, No. 3, pp. 28-32.

3. Ugolovnyy kodeks Rossiyskoy Federatsii ot 13 iyunya 1996 g. № 63-FZ [The Criminal Code of the Russian Federation dated June 13, 1996 No. 63-FZ]. *Sobraniye zakonodatel'stva RF* [*Collected Legislation of the Russian Federation*], 1996, No. 25, section 2954.

4. Postanovleniye Plenuma Verkhovnogo Suda RF ot 30 noyabrya 2017 g. № 48 «O sudebnoy praktike po delam o moshennichestve, prisvoyenii i rastrate» [Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48 "On judicial practice in cases of fraud, misappropriation and embezzlement"]. *Byulleten' Verkhovnogo Suda RF* [*Bulletin of the Supreme Court of the Russian Federation*], 2018, No. 2.

5. Grigoryan G.R. O sotsial'no-pravovoy sushchnosti korystnykh imushchestvennykh prestupleniy, sovershayemykh s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy [On the Socio-legal Nature of Self-serving Property Crimes Committed Using Information and Telecommunications Technologies]. *Rossiyskaya yustitsiya* [*Russian Justice*], 2020, No. 10, pp. 13-15.

6. Oleynik E.N. Ob"yekt moshennichestva s ispol'zovaniyem elektronnykh sredstv platezha [An Object of Fraud Using Electronic Payment Means]. *Ugolovnoye sudoproizvodstvo* [*Criminal Justice*], 2020, No. 3, pp. 45-48.

7. Makarov A.V., Shadrin D.A. K voprosu o kvalifikatsii khishcheniy s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy na ob"yektakh transporta (po materialam Zabaykal'skogo LU MVD Rossii na transporte) [On Qualification of Embezzlements Using Infor-

mation and Telecommunication Technologies at Transport Facilities (Based on Files of the Transbaikal Linear Transport Directorate of the Ministry of Internal Affairs of Russia)]. *Transportnoye pravo* [*Transport Law*], 2020, No. 3, pp. 17-21.

8. Opredeleniye Sudebnoy kollegii po ugolovnym delam Verkhovnogo Suda Rossiyskoy Federatsii ot 29 sentyabrya 2020 g. № 12-UDP20-5-K6. Tekst : elektronnyy [Determination of the Judicial Collegium for Criminal Cases of the Supreme Court of the Russian Federation dated September 29, 2020 No. 12-UDP20-5-K6. Text: electronic]. Konsul'tantPlyus: sayt [ConsultantPlus: site]. URL: http://www.consultant.ru (date of access: 28.11.2020).

9. Yani P.S. Khishcheniye s ispol'zovaniyem chuzhoy bankovskoy karty v magazine sleduyet kvalifitsirovat' kak moshennichestvo [Theft Committed with Use of a Someone Else's Bank Card in a Store to Classify as Fraud]. *Zakonnost'* [*Legality*], 2020, No. 12, pp. 39-43.

10. Filatova M.A. Khishcheniye s ispol'zovaniyem chuzhoy bankovskoy karty v magazine obrazuyet sostav krazhi [Theft Committed with Use of a Someone Else's Bank Card in a Store Constitutes Components of Larceny]. *Zakonnost'* [*Legality*], 2020, No. 12, pp. 34-38.

11. Pakharukov A.A. Primernaya osnovnaya obrazovatel'naya programma vysshego yuridicheskogo obrazovaniya kak model' realizatsii kompetentnostnogo podkhoda: voprosy pravovogo regulirovaniya [Exemplary Higher Legal Education Curriculum as a Model for Implementation of the Competency-based Approach: Issues of Legal Regulation]. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* [*Izvestiya of Irkutsk State Economics Academy*], 2016, Vol. 26, No. 1, pp. 115-122.

Информация об авторах

Воробьева Екатерина Романовна – магистрант, Иркутский государственный университет путей сообщения, 664074, г. Иркутск, ул. Чернышевского, 15, e-mail: e.konnova98@yandex.ru.

Крупская Александра Евгеньевна – магистрант, Иркутский государственный университет путей сообщения, 664074, г. Иркутск, ул. Чернышевского, 15, e-mail: 202099505@irgups.ru.

Authors

Vorobyova Ekaterina Romanovna – undergraduate, Irkutsk State Transport University, 15 Chernishevsky St., 664074, Irkutsk, Russia; e-mail: e.konnova98@yandex.ru.

Krupskaya Aleksandra Evgenievna – undergraduate, Irkutsk State Transport University, 15 Chernishevsky St., 664074, Irkutsk, Russia; e-mail: 202099505@irgups.ru.

Для цитирования

Воробьева Е. Р. Уголовно-правовая характеристика онлайн-мошенничества [Электронный ресурс] / Е. Р. Воробьева, А. Е. Крупская // Молодая наука Сибири: электрон. науч. журн. — 2020. — № 4. — Режим доступа: http://mnv.irgups.ru/toma/410-20, свободный. — Загл. с экрана. — Яз. рус., англ. (дата обращения: 12.12.2020).

For citation

Vorobyova E. R., Krupskaya A. E. Ugolovno-pravovaya kharakteristika onlayn-moshennichestva [Criminal Law Characteristics of Online Fraud]. Molodaya nauka Sibiri: ehlektronnyj nauchnyj zhurnal [Young science of Siberia: electronic scientific journal], 2020, No. 4. Access mode: http://mnv.irgups.ru/toma/410-20, free. Title from the screen. Languages: Russian, English [appeal date: 12.12.2020].