

# УГОЛОВНЫЙ ПРОЦЕСС

## Criminal Procedure

УДК 343.9:004

DOI: 10.19073/2658-7602-2022-19-2-156-164

EDN: DYEXOW



*Оригинальная научная статья*

### Вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий: криминалистический и уголовно-процессуальный аспекты

**Г. Д. Бадзгардзе** 

*Санкт-Петербургский юридический институт (филиал)*

*Университета прокуратуры Российской Федерации, Санкт-Петербург, Российская Федерация*

✉ [badzgarдзе98@gmail.com](mailto:badzgarдзе98@gmail.com)

**Аннотация.** Автор рассматривает некоторые дискуссионные вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий. В результате проведенного исследования делается вывод, что современное развитие уголовно-процессуального законодательства не позволяет в должной степени разрешить практические проблемы и коллизии, которые выражаются в неурегулировании вопросов определения места совершения мошенничества, предметом которого являются безналичные денежные средства, когда оно было осуществлено посредством нескольких банковских и небанковских переводов безналичных денежных средств в пользу преступника, и предлагается решение проблемы посредством указания в постановлении Пленума Верховного Суда от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», что местом совершения мошенничества, предметом которого выступают безналичные денежные средства, является местоположение (фактический адрес) финансовой организации (филиала, подразделения, представительства финансовой организации), в которой у потерпевшего был открыт счет и с которого была осуществлена последняя или наибольшая транзакция в преступных интересах субъекта преступления. Данные изменения, по мнению автора, позволят разрешить практические проблемы, возникающие при определении места предварительного расследования мошенничества, совершенного с использованием информационных технологий. Проводится анализ системы мест, которые можно считать местом совершения подобных мошенничеств, в криминалистическом смысле. Автор приходит к выводу, что среди таких мест можно выделить местонахождение преступника, местонахождение потерпевшего, а также местонахождение денежных средств потерпевшего, которые были обращены преступником в свою пользу. Результатом осуществленного анализа проблемы установления последнего места совершения мошенничества, осуществленного с использованием информационных технологий, является констатация отсутствия однозначных ответов, в связи с чем автор выражает надежду на получение не только конструктивных предложений, но и любых мнений, которые позволили бы приблизиться к ее решению.

**Ключевые слова:** безналичные денежные средства; место производства предварительного расследования; мошенничество, совершенное с использованием информационных технологий; киберпреступления; расследование киберпреступлений; противодействие киберпреступлениям; IT-преступления.

© Бадзгардзе Г. Д., 2022

Для цитирования: Бадзгардзе Г. Д. Вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий: криминалистический и уголовно-процессуальный аспекты // Сибирское юридическое обозрение. 2022. Т. 19, № 2. С. 156–164. DOI: <https://doi.org/10.19073/2658-7602-2022-19-2-156-164>. EDN: <https://elibrary.ru/dyexow>

*Original scientific article*

## Issues of Establishing the Place of Fraud Carried Out Using Information Technologies: Forensic and Criminal Procedure Aspects

**G. D. Badzgarдзе** 

*St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation, Saint Petersburg, Russian Federation*

✉ [badzgarдзе98@gmail.com](mailto:badzgarдзе98@gmail.com)

**Abstract.** The Author considers some debatable issues of establishing the place of fraud committed using information technology. The result of the study is the conclusion that the current development of criminal procedure legislation does not allow to adequately resolve practical problems and conflicts, which are expressed in the failure to resolve the issues of determining the place of committing fraud, the subject of which is non-cash funds, when it was carried out through several banking and non-banking transfers of non-cash funds in favor of the criminal, and proposes a solution to the problem by indicating in the decision of the Plenum of the Supreme Court dated November 30, 2017 No. 48 “On judicial practice in cases of fraud, misappropriation and embezzlement”, that the place of fraud, the subject of which are non-cash funds is the location (actual address) of the financial institution (branch, division, representative office of the financial institution), in which the victim had an account opened and from which the last or most transaction in the criminal interests of the subject of the crime. These changes, according to the Author, will allow solving practical problems that arise when determining the place of the preliminary investigation of fraud committed using information technology. An analysis is made of the system of places that can be considered a place of committing fraud using information technology, in a forensic sense. The Author comes to the conclusion that among such places one can single out the location of the offender, the location of the victim, as well as the location of the victim's funds, which were turned by the criminal in his favor. The result of the analysis of the problem of establishing the last place of committing fraud carried out using information technology is a statement of the absence of unequivocal answers, in connection with which the Author expresses the hope of receiving not only constructive suggestions, but also any opinions that would make it possible to get closer to its resolution.

**Keywords:** non-cash funds; place of preliminary investigation of fraud committed with the use of information technology, cybercrime, investigation of cybercrime, combating cybercrime, IT-crime.

**For citation:** Badzgarдзе G. D. Issues of Establishing the Place of Fraud Carried Out Using Information Technologies: Forensic and Criminal Procedure Aspects. *Siberian Law Review*. 2022;19(2):156-164. DOI: <https://doi.org/10.19073/2658-7602-2022-19-2-156-164>. EDN: <https://elibrary.ru/dyexow> (In Russ.).

### ВВЕДЕНИЕ

Непрекращающееся изменение общественных отношений в развитых государствах приводит к все большей цифровизации денежного обращения, ин-

форматизации и интеграции информационных технологий в жизнь и деятельность человека [1–2]. Данные процессы закономерно приводят к «перепрофилированию» деятельности преступного элемента,

что выражается в сокращении числа хищений, связанных с реальным контактом преступника и потерпевшего, и возрастании «виртуальных» связей между ними [3–5].

Об этом свидетельствуют и статистические данные о преступности в России за 2020 и 2021 гг. В 2020 г. количество краж сократилось на 3 %, грабежей – на 16,2 %, разбоев – на 21,7 %<sup>1</sup>. Подобная тенденция сохранилась и в 2021 г.: количество краж уменьшилось на 2,4 %, грабежей – на 18,1 %, разбоев – на 16 %<sup>2</sup>. При этом в последние годы наблюдается галопирующее возрастание числа совершаемых хищений с использованием информационных технологий, особенно мошенничества, предусмотренного ст.ст. 159, 159<sup>3</sup>, 159<sup>6</sup> Уголовного кодекса Российской Федерации (далее – УК РФ). В совокупности за 2020 и 2021 гг. количество преступлений, предусмотренных ст. 159 УК РФ, совершенных с использованием информационных технологий, увеличилось на 98,96 %; предусмотренных ст. 159<sup>3</sup> УК РФ – уменьшилось на 57,14 % (однако в 2019 г. количество данных преступлений увеличилось на 280 %<sup>3</sup>), предусмотренных ст. 159<sup>6</sup> – уменьшилось на 59,4 %.

Увеличение числа преступлений, совершенных с использованием информационных технологий, обусловило рост тяжкой преступности в России. И как справедливо отметил Министр внутренних дел России В. А. Колокольцев, к этому привело именно резкое увеличение числа мошенничеств в телекоммуникационных сферах<sup>4</sup>.

Противодействие мошенничеству, совершенному с использованием информационных технологий, осложняется

не только количеством данных преступлений, но и способностью правоохранительных органов осуществлять деятельность по их раскрытию и расследованию. О неблагополучии в данной области свидетельствуют статистические данные раскрываемости рассматриваемых категорий преступлений. Так, за 2021 г. было раскрыто 21 610 из 240 117 преступлений рассматриваемой категории, что составляет всего 9 %. Более того, доля раскрываемых преступлений в сравнении с 2020 г. только уменьшилась.

Причин указанной низкой эффективности правоохранительных органов в рассматриваемой сфере много, и в качестве одной из наиболее существенных следует выделить проблему установления места совершения преступления, которую мы хотели бы рассмотреть в рамках настоящего исследования [6].

Место совершения любого преступления можно рассматривать с точки зрения криминалистики и с точки зрения уголовно-процессуального права. При этом примечательно, что именно при расследовании мошенничества, совершенного с использованием информационных технологий, столкновение этих двух юридических наук приводит к серьезным практическим проблемам, усложняющим процесс установления истины по уголовному делу.

### **УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ АСПЕКТ ОПРЕДЕЛЕНИЯ МЕСТА ОСУЩЕСТВЛЕНИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

С позиции уголовно-процессуального права проблема, связанная с местом

<sup>1</sup> *Состояние преступности в России за январь–декабрь 2020 года*. М. : М-во внутр. дел Рос. Федерации ФКУ «Главный информационно-аналитический центр», 2020. С. 4.-

<sup>2</sup> *Состояние преступности в России за январь–декабрь 2021 года*. М. : М-во внутр. дел Рос. Федерации ФКУ «Главный информационно-аналитический центр», 2021. С. 3.

<sup>3</sup> *Состояние преступности в России за январь–декабрь 2019 года*. М. : М-во внутр. дел Рос. Федерации ФКУ «Главный информационно-аналитический центр», 2021. С. 31.

<sup>4</sup> *Владимир Александрович Колокольцев // Офиц. сайт М-ва внутр. дел Рос. Федерации*. URL: <https://xn--b1aew.xn--p1ai/speech/item/22548863/>

совершения преступления, выражается в определении подследственности в соответствии с нормами ст. 152 УПК РФ [7]. В соответствии с указанной нормой, по общему правилу, предварительное расследование производится по месту совершения преступления. При этом, как указывается в п. 5 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», местом совершения мошенничества, состоящего в хищении безналичных денежных средств (а именно они, как правило, и являются предметом совершения мошенничества с использованием информационных технологий) выступает «место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета»<sup>5</sup> [8].

Представляется, что разъяснения Верховного Суда в части, касающейся установления места совершения мошенничества, не соответствуют практическим потребностям, возникающим при производстве проверки сообщения о преступлении и предварительного расследования по уголовным делам о мошенничестве, совершенном с использованием информационных технологий [9]. Особенностью совершения данного преступления является то, что денежные средства потерпевшего могут изыматься не с одного счета в одном банке, но и с нескольких счетов в нескольких банках и (или) небанковских организациях, предоставляющих услуги по хранению цифровых денежных средств (WebMoney, ЮMoney, QIWI Кошелек и др.). Подобные преступные действия охвачены единым умыслом, направленным на хищение имущества путем обмана или злоупотребления доверием с использованием информационных технологий,

однако достоверно установить место совершения преступления, исходя из положений вышеупомянутого постановления Пленума Верховного Суда, не представляется возможным, поскольку денежные средства перечисляются не с одного банковского счета, а с нескольких. В качестве примера можно привести приговор Приволжского районного суда города Казани № 1-333/2018 1-9/2019 от 26 июня 2019 г. по делу № 1-333/2018 в отношении Мухтарова Р. Г., осуществлявшего мошенническую деятельность посредством заключения договоров подряда и поставки мебели через заблаговременно созданные сайт в сети «Интернет» и электронные почты без цели дальнейшего исполнения гражданско-правовых обязательств. По одному из эпизодов мошенничества в приведенном приговоре суда не установлено место совершения преступления; указывается место нахождения преступника в момент его совершения, указывается, что часть суммы, направленной на приобретение мебели потерпевшим, была переведена через терминал оплаты «Колибри»; часть суммы направлена через мобильное приложение ПАО «ВТБ» на счет приема интернет-платежей ООО РНКО «Единая Касса», открытый на имя осужденного. Подобные излишние формулировки суда, описывающие место совершения преступления, по нашему мнению, указывают на фактическую невозможность его четкого определения. При этом из вышеуказанного постановления Пленума Верховного Суда прямо следует, что в приведенном случае имеется два полноценных места совершения преступления: местонахождение терминала оплаты «Колибри» и филиала (представительства) ПАО «ВТБ», в котором открыт банковский счет.

Как справедливо указывает Ю. В. Павлюченко, подобные проблемы определения места совершения преступления,

---

<sup>5</sup> О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда Рос. Федерации от 30 нояб. 2017 г. № 48 (ред. от 29 июня 2021 г.) // Рос. газ. 2017. 11 дек.

предметом которых являются безналичные денежные средства, часто приводят к неправильному определению подследственности и подсудности, что разрешается в лучшем случае на стадии апелляционного производства, а значит, противоречит принципам разумности сроков уголовного процесса и процессуальной экономии [10].

### **МЕСТО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ, СВЯЗАННОЕ С ДЕЯТЕЛЬНОСТЬЮ БАНКА**

Определение места совершения мошенничества, осуществленного с использованием информационных технологий, имеет важное криминалистическое значение и ряд особенностей. По существу, место совершения преступления с позиции уголовно-процессуального права представляет собой лишь один из элементов системы мест совершения мошенничества с использованием информационных технологий с позиции криминалистики.

Как нами указывалось ранее, в уголовно-процессуальном смысле местом совершения преступления будет местонахождение банковской организации, в которой у потерпевшего открыт счет и в котором находятся безналичные денежные средства. Однако если мы исходим из буквального толкования, что местом совершения преступления является место, где оно было совершено, то как им может признаваться место, в котором в соответствующее время отсутствовали и потерпевший, и преступник?

Углубляясь в правовую природу предмета преступления, нельзя не коснуться положений гражданского права, которые определяют юридический статус безналичных денежных средств. В соответствии со ст. 845 Гражданского кодекса Российской Федерации (далее – ГК РФ) денежные средства, перечисленные на счет, находятся в распоряжении банка. Владелец же счета, исходя из положений ст.ст. 861 и 862 ГК РФ, вправе давать обя-

зательные для банка указания об осуществлении расчетов безналичными денежными средствами, хранящимися на счете, в формах поручения, расчетов по аккредитиву, по инкассо, чеками и иными формами, установленными банковскими правилами или применяемыми в банковской практике обычаями, а банк в свою очередь имеет право распоряжаться денежными средствами, переданными ему по договору банковского счета (банковского вклада и т. п.) [11].

Соответственно и мошенничество, совершенное с использованием информационных технологий, реализуется путем осуществления потерпевшим одного из вышеупомянутых указаний банку о совершении действий по переводу безналичных денежных средств в пользу преступника на его банковский или иной счет. Как правило, при мошенничестве, совершаемом с использованием информационных технологий, потерпевший дает дистанционные указания банку в форме поручений, из чего и следует, что на месте совершения преступления в уголовно-процессуальном смысле он не находится.

Более того, подразделение банка или иной организации, в которой у потерпевшего открыт банковский счет, нельзя считать полноценным местом совершения преступления, поскольку там не будет никаких его следов. По сути, месторасположение подразделения банка представляет собой всего лишь помещение, в котором банк осуществляет свою финансовую деятельность. Местом же хранения безналичных денежных средств, исходя из их технологической природы, будет выступать сервер системы хранения данных, расположенный в центре обработки данных (дата-центре).

Как правило, распоряжение переданными денежными средствами выражается в предоставлении кредитов различным лицам. При этом является очевидным то обстоятельство, что после указанных

действий банк фактически производит дополнительные безналичные денежные средства, налично подкрепленные суммой, значительно меньшей суммы безналичных денежных средств. Данное обстоятельство следует из того, что при передаче денежных средств владельцем счета банку он не теряет права их востребовать. Тогда как должник, взявший в кредит денежные средства, которыми распоряжается банк, приобретает право владения и распоряжения ими.

Поскольку наличные денежные средства владельца счета передаются банком в пользование и распоряжение должнику, то в зависимости от последующих условий хранения должником кредитных денежных средств местом нахождения денежных средств владельца банковского счета может быть как место, в котором банк хранит наличные (если мы исходим из того, что безналичные средства должны быть подтверждены наличными), либо место, определяемое должником банка (если денежные средства, переданные в кредит клиенту банка были им в последствии обналичены).

Если исходить из того, что местом нахождения безналичных денежных средств, являющихся предметом мошенничества, совершенного с использованием информационных технологий, является центр обработки данных (дата-центр), в котором находится система хранения данных, с определенной долей условности, состоящая из серверов, то ситуация усложняется тем, что следы преступных действий находятся не в дата-центре, а в сервере, расположенном в нем. При этом закодированные безналичные деньги перенаправляются посредством дачи дистанционного поручения банку в пользу преступника. В свою очередь банк (иная финансовая организация, предоставляющая услуги по переводу безналичных денежных средств) проверяет по формальным признакам правомерность исполнения данного дистан-

ционного поручения. В силу огромного количества подобных поручений проверка их правомерности достигается с минимальным человеческим участием – путем использования автоматизированного программного обеспечения, сущностью которого является изменение информации, содержащейся на электронных банковских счетах лица, дающего банковской (финансовой) организации поручение, и лица, в интересах которого дается это поручение. В указанном случае местом совершения преступления может выступать и местонахождение соответствующей электронно-вычислительной машины, на которой предустановлено соответствующее программное обеспечение, с помощью которого выполняются вышеупомянутые вычислительные операции.

На основании изложенного, автор вынужден признать, что не находит способа разрешения вопроса об определении места совершения преступления в криминалистическом понимании применительно к месту отчуждения принадлежащих потерпевшему безналичных денежных средств в пользу преступника, совершающего мошенничество с использованием информационных технологий.

#### **МЕСТОНАХОЖДЕНИЕ ПРЕСТУПНИКА И ПОТЕРПЕВШЕГО КАК МЕСТО МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Одним из мест совершения мошенничества с использованием информационных технологий является место нахождения преступника в момент совершения преступления.

В связи с тем, что при совершении мошенничества с использованием информационных технологий, как правило, преступник и потерпевший находятся в разных местах, небезосновательно утверждение, что среди мест совершения рассматриваемой категории преступлений

нужно также выделить место нахождения потерпевшего.

При этом важно отметить, что современный уровень развития средств связи позволяет лицу в момент совершения преступления менять место нахождения, например, посредством удаленного доступа к другому устройству, находящемуся по иному адресу. Однако в силу того, что следы мошенничества, совершенного с использованием информационных технологий, чаще всего являются цифровыми, под местом нахождения преступника в криминалистическом смысле считается система мест, в которых он находился в ходе совершения преступления, и использовал информационные технологии для достижения преступных целей. Ситуация существования множественности мест преступления может усложняться в случае использования преступником в целях сокрытия следов преступления программного обеспечения для удаленного доступа и контроля компьютеров, обмена файлами между управляющей и управляемой машинами (TeamViewer, AnyDesk и др.). Данное программное обеспечение позволяет преступнику, находясь в отдаленном месте, давать с одного технического устройства удаленные команды другому техническому устройству по производству практически всего спектра возможных действий, осуществляемого последним устройством. Данные действия не требуют использования программного обеспечения, гарантирующего защищенные соединения, предоставляющие анонимность, однако не исключают его.

В свою очередь местом нахождения потерпевшего будет являться система мест, в которых он находился в ходе совершения мошенничества и использовал информационные технологии при взаимодействии с преступником.

Если же мошенничество с использованием информационных технологий было совершено без дистанционного контакта

преступника с потерпевшим в цифровой среде (данные ситуации возникают, когда преступник получает доступ к цифровым сервисам потерпевшего в сети Интернет без ведома последнего), то с криминалистической точки зрения местом преступления, связанным с потерпевшим, будет выступать местонахождение технического устройства, с которого он получал доступ для использования цифровых сервисов, хранящих цифровые активы, похищенные преступником.

### **ЗАКЛЮЧЕНИЕ**

Вышеизложенное, на наш взгляд, служит достаточным обоснованием внесения изменения в п. 5 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», где указать, что местом совершения мошенничества, предметом которого выступают безналичные денежные средства, является местоположение (фактический адрес) финансовой организации (филиала, подразделения, представительства финансовой организации), в которой у потерпевшего был открыт счет и с которого была осуществлена последняя или наибольшая транзакция в преступных интересах субъекта преступления. Данные изменения, по нашему мнению, позволят разрешить практические проблемы, возникающие при определении места предварительного расследования мошенничества, совершенного с использованием информационных технологий.

Кроме того, в связи с особенностями способа совершения и предмета мошенничества с использованием информационных технологий, а также характера оставляемых при этом следов, с криминалистической точки зрения существует система мест совершения мошенничества, совершенного с использованием информационных технологий. Данную систему можно представить

в виде местонахождения потерпевшего, местонахождения преступника, а также места, в котором хранились ценности потерпевшего и из которого они были направлены в пользу преступника.

При этом местонахождение как преступника, так и потерпевшего связано с местом нахождения технических средств, посредством использования которых они взаимодействовали друг с дру-

гом. Если же личностное взаимодействие преступника и потерпевшего отсутствовало, то местом совершения преступления с криминалистической точки зрения и применительно к потерпевшему будет являться местонахождение технического устройства, с которого потерпевшим осуществлялся доступ к цифровым сервисам, хранящим информационно-электронные активы.

### Список литературы

1. Шувалова М. А. Осознание необходимости применения инновационных технологий в уголовном процессе // *Юридическая наука: история и современность*. 2021. № 1. С. 133–139.
2. Зазулин А. И. Функции цифровой информации и технологий в уголовном процессе // *Сибирское юридическое обозрение*. 2020. Т. 17, № 1. С. 75–82. DOI: <https://doi.org/10.19073/2658-7602-2020-17-1-75-82>
3. Филиппов А. Р. Феномен мошенничества в России XXI века: уголовно-правовая, криминологическая и социально-психологическая характеристика // *Юридическая наука: история и современность*. 2021. № 6. С. 134–146.
4. Старостенко О. А. Закономерности становления и развития кибермошенничества в России и за рубежом // *Вестник Уральского юридического института МВД России*. 2021. № 1 (29). С. 138–143.
5. Грачева Ю. В. Цифровые технологии и безопасность личности // *Криминалист*. 2019. № 1 (26). С. 25–29.
6. Баркалова Е. В., Ручкин К. В., Серова Е. Б. Актуальные вопросы уголовного преследования за совершение мошенничества с использованием информационно-телекоммуникационных технологий // *Криминалист*. 2021. № 3 (36). С. 57–64.
7. Костюк М. Ф., Басырова З. Р. Преступления против собственности с использованием цифровых технологий // *Юридическая наука: история и современность*. 2021. № 9. С. 154–159.
8. Степанова М. А., Царёв Е. В. Проблемы определения места совершения хищения денежных средств, с использованием информационно-телекоммуникационных технологий // *Вестник Белгородского юридического института МВД России имени И. Д. Путилина*. 2021. № 1. С. 12–16.
9. Хайдаров А. А. Дистанционное мошенничество. Расследование преступления и доказывание в суде // *Уголовный процесс*. 2020. № 10. С. 24–35.
10. Павлюченко Ю. В. Место совершения преступления и момент его окончания по делам о мошенничестве в отношении безналичных денежных средств // *Уголовное право*. 2018. № 2. С. 69–78.
11. Савченко М. М. Правовая природа безналичных денежных и электронных денег как предмета преступных посягательств // *Бизнес. Образование. Право*. 2021. № 2 (55). С. 244–250. DOI: <https://doi.org/10.25683/VOLBI.2021.55.235>

### References

1. Shuvalova M. A. Awareness of the Need to Use Innovative Technologies in Criminal Proceedings. *Juridical Science: History and Modernity*. 2021;1:133–139. (In Russ.).
2. Zazulin A. I. Functions of Digital Information and Technologies in Criminal Proceedings. *Siberian Law Review*. 2020;17(1):75-82. <https://doi.org/10.19073/2658-7602-2020-17-1-75-82> (In Russ.).
3. Filippov A. R. The Phenomenon of Fraud in Russia of the XXI Century: Criminal-Legal, Criminological and Socio-Psychological Characteristics. *Juridical Science: History and Modernity*. 2021;6:134-146. (In Russ.).
4. Starostenko O. A. Regularities of the Formation and Development of Cyber Fraud in Russia and Abroad. *Bulletin of the Ural Law Institute of the Ministry of the of the Interior of the Russian Federation*. 2021;1:138-143. (In Russ.).
5. Gracheva Yu. V. Digital Technologies and Personal Security. *Criminalist*. 2019;1:25-29. (In Russ.).
6. Barkalova E. V., Ruchkin K. V., Serova E. B. Current Issues of Criminal Prosecution for Commission of Fraud with the Use of Information and Communication Technologies. *Criminalist*. 2021;3:57-64. (In Russ.).
7. Kostyuk M. F., Basyrova Z. R. Digital Property Crimes. *Juridical Science: History and Modernity*. 2021;9:154-159. (In Russ.).
8. Stepanova M. A., Tsarev E. V. Problems of Determining the Place of Embezzlement of Funds Using Information and Telecommunications Technologies. *Vestnik of Putilin Belgorod Law Institute of Ministry of the Interior of Russia*. 2021;1:12-16. (In Russ.).

9. Khaydarov A. A. Remote Fraud. Investigation and Evidence. *Criminal Procedure*. 2020;10:24-35. (In Russ.).
10. Pavlyuchenko Yu. V. Crime Scene and Its Commission End-Time on Fraud Cases in Relation To Wire Funds Transfers. *Ugolovnoe pravo*. 2018;2:69-78. (In Russ.).
11. Savchenko M. M. The Legal Nature of Non-Cash and Electronic Money as a Subject of Criminal Encroachments. *Business. Education. Right*. 2021;2:244-250. DOI: <https://doi.org/10.25683/VOLBI.2021.55.235> (In Russ.).

#### ИНФОРМАЦИЯ ОБ АВТОРЕ

**Георгий Давидович Бадзгардзе**, аспирант кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации (Литейный пр., 44, Санкт-Петербург, 191104, Российская Федерация); ORCID: <https://orcid.org/0000-0001-7550-1430>; e-mail: [badzgaradze98@gmail.com](mailto:badzgaradze98@gmail.com)

#### ABOUT THE AUTHOR

**Georgiy D. Badzgaradze**, Postgraduate Student of the Department of Criminal Procedure and Forensic Science at the St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation (44 Liteiny pr., St. Petersburg, 191104, Russian Federation); ORCID: <https://orcid.org/0000-0001-7550-1430>; e-mail: [badzgaradze98@gmail.com](mailto:badzgaradze98@gmail.com)

Поступила | Received  
04.05.2022

Поступила после рецензирования  
и доработки | Revised  
17.06.2022

Принята к публикации | Accepted  
20.06.2022