Научная статья
УДК 343.2
EDN DLNAFD
DOI 10.17150/2500-4255.2025.19(2).160-172

ОБМАННОЕ ВОЗДЕЙСТВИЕ НА КОМПЬЮТЕРНУЮ СИСТЕМУ КАК СПОСОБ ХИЩЕНИЯ

К.В. Ображиев
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация

Информация о статье

Дата поступления
10 марта 2025 г.

Дата принятия в печать
9 июня 2025 г.

Дата онлайн-размещения
17 июня 2025 г.

Ключевые слова

Обманное воздействие; мошеннический обман; мошенничество; обман компьютерной системы; мошенничество в сфере компьютерной информации; компьютерное хищение; статья 159 УК РФ; статья 159.6 УК РФ

Аннотация. Традиционная уголовно-правовая трактовка мошенничества не позволяет признать мошенническим обманом воздействие на компьютерную систему. В настоящее время это положение подвергается ревизии, поскольку в условиях цифровизации и автоматизации экономических процессов полномочия по принятию юридически значимых решений, связанных с распоряжением имуществом, все чаще передаются от человека компьютерным системам (зачисление на банковский счет денежных средств, внесенных через банкомат, обработка распоряжений о переводе денежных средств, выдача потребительского кредита и т.п.).

Основываясь на традиционной интерпретации мошеннического обмана, доктрина предлагает дифференцированный подход к квалификации хищений, совершаемых посредством предоставления заведомо ложной информации: если виновный вводит в заблуждение человека (например, сотрудника банка), то содеянное надлежит квалифицировать как мошенничество; если же ложная информация обрабатывается компьютерной программой, которая в автоматическом режиме принимает решение о перечислении денежных средств (например, скоринговой системой банка), то рекомендуется вменять состав кражи с банковского счета. Обоснованность такого подхода вызывает сомнения, поскольку он: игнорирует направленность умысла виновного на хищение путем обмана, ставит квалификацию преступления в зависимость от факторов, которые находятся вне сферы интеллектуально-волевого контроля злоумышленника; порождает существенные, но при этом ничем не оправданные различия в наказуемости деяний; не согласуется с общепринятыми критериями разграничения форм хищения.

В поиске решения обозначенной проблемы автор обращается к зарубежному опыту, анализируя основные подходы к уголовно-правовому противодействию хищениям, совершаемым путем обманного воздействия на компьютерную систему; оценивает достоинства и недостатки отечественного уголовного законодательства; констатирует, что ст. 159.6 УК РФ, специально сконструированная для борьбы с рассматриваемыми видами хищений, свое предназначение не выполняет, что побуждает правоприменителей к расширительной трактовке мошеннического обмана.

В стремлении обеспечить адекватную уголовно-правовую оценку анализируемых видов хищений суды, лишенные возможности применять ст. 159.6 УК РФ, приравнивают обманное воздействие на компьютерную систему к обману человека, что подтверждается анализом ряда судебных актов. Таким образом, после резкого ограничения сферы применения ст. 159.6 УК РФ, состоявшегося в 2017 г., правоприменительная практика постепенно разворачивается в сторону широкой трактовки мошеннического обмана, подобной той, что используется в британском Акте о мошенничестве 2006 г.

ISSN 2500-1442

Original article

FRAUDULENT INFLUENCE ON A COMPUTER SYSTEM AS A METHOD OF THEFT

Konstantin V. Obrazhiev
Kutafin Moscow State Law University (MSAL), Moscow, the Russian Federation

Article info

Received
2025 March 10

Accepted
2025 June 9

Available online
2025 June 17

Keywords

Deceptive influence; fraudulent deception; fraud; deception of a computer system; fraud in the field of computer information; computer theft; Article 159 of the Criminal Code of the Russian Federation; Article 159.6 of the Criminal Code of the Russian Federation

Abstract. The traditional criminal law interpretation of fraud does not allow for recognizing impact on a computer system as fraudulent deception. This clause is being currently revised, since in the condition of digitization and automation of economic processes the authority to make legally valid decisions involving property is increasingly often delegated not to humans, but to computer systems (crediting a bank account with cash deposited at ATMs, processing orders to transfer money, issuing consumer loans, and so on).

Using the traditional interpretation of fraudulent deception, the doctrine offers a differentiated approach to the qualification of theft committed by providing deliberately false information: if the perpetrator deliberately misleads a human (for example, a bank employee), these actions should be qualified as fraud; if the false information is processed by computer software that makes a decision regarding the transfer of money automatically (for example, the scoring system of a bank), then it is recommended to impute the crime of theft from a bank account. The feasibility of such an approach raises certain doubts since it: ignores the intent of the perpetrator to commit theft through deception and makes the qualification of the crime dependent on the factors outside the intellectual and volitional control of the culprit; gives rise to considerable but unjustified differences in the punishments for crimes; does not agree with the conventional criteria for differentiating between forms of theft.

While searching for a solution to this problem, the author turns to foreign experience and analyses key approaches to criminal law counteraction to theft committed through a fraudulent influence on a computer system; assesses the advantages and disadvantages of Russian criminal legislation; states that Art. 159.6 of the Criminal Code of the Russian Federation, especially written to counteract the thefts under analysis, does not perform its function, which makes law enforcers use a broad interpretation of fraudulent deception.

Trying to provide an adequate criminal law assessment of the types of theft under analysis, the courts, derived of an opportunity to use Art. 159.6 of the Criminal Code of the Russian Federation, equal fraudulent influence on a computer system and deception of a person, which is proven by the analysis of a number of court acts. Thus, after a sharp limitation of the sphere of application for Art. 159.6 of the Criminal Code of the Russian Federation which took place in 2017, the law enforcement practice is gradually moving towards a broad interpretation of fraudulent deception similar to that used in the UK Fraud Act 2006.

1. Традиционная уголовно-правовая трактовка мошенничества не позволяет признать мошенническим обманом воздействие на компьютерную или иную технологическую систему, функционирующую в автоматическом режиме. Впрочем, аксиоматичное положение о том, что «компьютер, как и замок у сейфа, нельзя обмануть, поскольку технические устройства лишены психики»[1] [1, с. 42], в реалиях современной цифровой экономики все чаще ставится под сомнение.

Так, П.С. Яни в 2008 г. предположил, что по мере распространения различных идентификационных технических средств «судебная практика может склониться к тому, чтобы видеть в такого рода «обмане» идентификационной машины разновидность обмана как признака мошенничества» [5, с. 13]. Более категорично по этому поводу высказывается М.Н. Шипунова. Она предлагает в соответствующих случаях использовать юридическую фикцию, «при которой действия, связанные с предоставлением недостоверных сведений цифровому агенту (компьютерной системе с искусственным интеллектом) компании, будут признаваться обманом в уголовно-правовом смысле» [6, с. 47–52].

[1] Этот тезис в том или ином виде воспроизводится во всех крупных работах, посвященных преступлениям против собственности. См.: [2, с. 112; 3, с. 278, 345–346; 4, с. 186].

Подобная трансформация подходов к пониманию мошеннического обмана не случайна, ведь в условиях цифровизации и автоматизации экономических процессов полномочия по принятию юридически значимых решений, связанных с распоряжением имуществом, все чаще передаются от человека компьютерным системам[2]. В частности, подобные технологии активно используются для осуществления стандартизированных рутинных операций по взаимодействию с потребителями (зачисление на банковский счет денежных средств, внесенных через банкомат, обработка распоряжений о переводе денежных средств, выдача потребительского кредита и т.п.).

2. Весьма показательной в этом отношении можно считать сферу розничного онлайн-кредитования: крупные банки уже не первый год применяют автоматизированные банковские системы, которым делегированы не только проверка заемщика и оценка кредитных рисков, но и принятие решения о выдаче кредита [8, с. 34–42; 9; 10]. Подобные технологические решения оптимизируют банковскую деятельность, но они, к сожалению, не препятствуют совершению хищений кредитных средств, поскольку компьютерная программа далеко не во всех случаях способна распознать обман в личности и намерениях заемщика. В этом плане компьютерная система уязвима не меньше, чем человек.

Для дистанционного хищения денежных средств, предоставляемых банком на кредитной основе, в подавляющем большинстве случаев используется обман: если злоумышленник оформляет заявку на получение кредита от своего имени, изначально не намереваясь осуществлять платежи по его обслуживанию, то это типичный обман в намерениях; если же он авторизуется в программе интернет-банкинга (в мобильном банковском приложении), используя чужие конфиденциальные данные, и подает заявку на кредит от имени другого лица, то к обману в намерениях добавляется обман в личности.

Если решение о выдаче кредита принято сотрудником банка, то проблем с квалификацией содеянного не возникает — хищение кредитных средств квалифицируется как мошенничество: по ст. 159.1 УК РФ (при условии, что мошенник подал заявку через свой личный кабинет) или по ст. 159 УК РФ (если он действовал под чужим именем)[3]. Но в тех случаях, когда обработка внесенных в заявку заведомо ложных сведений и принятие решения о выдаче кредита осуществлялись в автоматическом режиме без участия сотрудников банка, информационное воздействие на психику человека отсутствует, вследствие чего большинство представителей уголовно-правовой доктрины полагают невозможным квалифицировать подобные хищения кредитных средств в качестве мошенничества. А поскольку ст. 159.6 УК РФ в этих случаях также неприменима (ведь изъятие денежных средств у банка производится без «взлома» компьютерных программ), то содеянное предлагается «по остаточному принципу» квалифицировать как кражу с банковского счета [11, с. 15–19; 12, с. 3–13].

Таким образом, основываясь на традиционной интерпретации мошеннического обмана, доктрина предлагает дифференцированный подход к квалификации хищений, совершаемых посредством дистанционного оформления кредита: если виновный вводит в заблуждение сотрудника банка, то содеянное надлежит квалифицировать как мошенничество; если же заявка на получение кредита обрабатывается специальной компьютерной программой в автоматическом режиме, то необходимо вменять кражу с банковского счета[4].

3. Обоснованность такого подхода вызывает серьезные сомнения, поскольку он идет вразрез с принципом субъективного вменения, игнори-

[2] С.А. Петров оговаривает, что компьютерная программа работает по заложенному в нее алгоритму, в связи с чем о «принятии решения» в этих случаях «можно говорить лишь условно, так как это мыслительный процесс, а компьютер не обладает разумом» [7, с. 47–51]. Но в правовом смысле это именно «решение», поскольку оно влечет юридически значимые последствия.

[3] В постановлении Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняется, что в случаях, когда в целях хищения денежных средств лицо, например, выдавало себя за другое, представив при оформлении кредита чужой паспорт, либо действовало по подложным документам от имени несуществующего физического или юридического лица, либо использовало для получения кредита иных лиц, не осведомленных о его преступных намерениях, основание для квалификации содеянного по ст. 159.1 УК РФ отсутствует, ответственность виновного наступает по ст. 159 УК РФ (п. 14).

[4] Практическую реализацию этого подхода см.: определение Шестого кассационного суда общей юрисдикции от 16.11.2022 № 77-5724/2022; определение Шестого кассационного суда общей юрисдикции от 28.02.2024 № 77-727/2024. Здесь и далее приведены ссылки на судебные решения, размещенные в справочно-правовой системе «КонсультантПлюс».

рует направленность умысла виновного на хищение путем обмана, ставит квалификацию преступления в зависимость от факторов, которые находятся вне сферы интеллектуально-волевого контроля злоумышленника (в частности, от механизма обработки заявки о получении кредита). Банки неохотно афишируют внутренние регламенты финансово-кредитной деятельности[5], вследствие чего злоумышленник, равно как и добросовестный заемщик, обратившийся в банк с заявкой о выдаче онлайн-кредита, как правило, не имеет представления о том, кто именно — человек или автоматизированная система — принимает решение по его заявке. Объективное вменение в анализируемых ситуациях, конечно же, недопустимо. Действия преступника следует квалифицировать с учетом направленности его умысла и избранного им обманного способа совершения преступления, не увязывая уголовно-правовую оценку с механизмом обработки ложной информации, внесенной им в электронную заявку на получение кредита.

Помимо этого, нельзя не учитывать, что дифференцированная уголовно-правовая оценка дистанционных хищений, основанных на обмане, порождает существенные, но при этом ничем не оправданные различия в наказуемости деяний (о диспропорциях в санкциях норм об ответственности за тайное и обманное хищение с банковского счета говорилось уже не раз). В частности, максимальное наказание за единолично совершенное мошенническое хищение кредитных средств в размере до 250 тыс. рублей по ч. 1 ст. 159 УК РФ составляет 2 года лишения свободы, а по ч. 1 ст. 159.1 УК РФ — 2 года принудительных работ, в то время как за кражу с банковского счета по п. «г» ч. 3 ст. 158 УК РФ предусмотрено наказание до 6 лет лишения свободы.

Социально-правовые основания для подобной дифференциации ответственности отсутствуют, ведь степень общественной опасности хищения кредитных средств не зависит от механизма обработки ложной информации, предоставленной похитителем. Тот факт, что электронная заявка, содержащая ложные сведения о личности и (или) намерениях заемщика, обработана компьютерной системой, а не сотрудником банка, нисколько не повышает общественную опасность хищения. Ее степень не меняется от субъекта восприятия недостоверных данных. Даже если преступник, желающий похитить денежные средства, лично явится в офис банка для получения кредита, то сообщенные им ложные сведения все равно будут внесены в специализированную компьютерную систему для скоринговой оценки заемщика, и именно компьютерная система примет решение о выдаче кредита или об отказе от его выдачи. Сотрудник банка, непосредственно взаимодействующий с недобросовестным заемщиком, в этом случае выполняет исключительно технические функции: вносит анкетные данные, запрашиваемую сумму кредита, выводит на печать кредитный договор и передает его заемщику для ознакомления и подписания. Следовательно, для принципиально различной квалификации хищений кредитных средств в зависимости от способа обработки заведомо ложных данных нет необходимых предпосылок.

Основным критерием разграничения форм хищения выступает способ совершения преступления, в котором концентрированно воплощаются объективные и субъективные факторы, определяющие степень общественной опасности хищения. В рассматриваемых случаях преступник осознанно избирает и реализует именно обманный способ совершения хищения, и никакие внешние факторы, не зависящие от виновного (в том числе механизм обработки ложной информации, предоставленной в целях хищения кредитных средств), не меняют сути выбранного способа, не превращают обманное хищение в тайное. Механизм обработки электронной заявки на получение кредита характеризует обстановку совершения хищения, специфику развития причинной связи между действиями виновного и наступившими последствиями (прямая причинная связь или связь, опосредованная работой компьютерной системы), но не способ преступления.

При дистанционном оформлении заявки на кредит обман в личности заемщика и (или) в его намерениях нельзя считать лишь приготовительным действием, облегчающим последующее тайное хищение кредитных средств. Никаких иных действий-способов, помимо обмана, виновный более не совершает, и автоматизированный режим обработки электронной заявки на получение кредита не способен перечеркнуть это обстоятельство. Перевод кредитных средств на подконтрольный виновному банковский счет,

[5] По словам первого заместителя председателя правления Сбербанка К. Царева, «часть банковских продуктов уходит «под капот», то есть клиенту в принципе не важно, как процесс устроен, ему важно получить услугу здесь и сейчас» [10].

совершаемый при дистанционном оформлении кредита от чужого имени, находится за рамками объективной стороны состава преступления, поскольку с момента списания денежных средств со счета банка хищение юридически окончено и ущерб потерпевшему (банку) уже причинен[6]. Следовательно, направляя электронную заявку на получение кредита, содержащую заведомо ложную информацию, злоумышленник начинает выполнять объективную сторону хищения, причем хищения обманного.

Говорить о тайности хищения здесь неуместно, поскольку банк не просто выполняет обязательное распоряжение о списании денежных средств, а *принимает решение о выдаче кредита на основании проверки заемщика и сведений, внесенных им в заявку на получение кредита.* Осуществление такой проверки (в ручном или в автоматическом режиме — без разницы) означает, что денежные средства перечислены на кредитной основе *под воздействием заведомо ложных данных,* а не тайно похищены.

4. Следует отметить, что затронутая проблема касается не только дистанционных хищений кредитных средств, совершаемых путем предоставления недостоверных данных. Посредством обманного воздействия на компьютерную систему совершаются хищения, совершаемые путем внесения в банкомат поддельных денежных купюр, изготовленных по методу аппликации (склейки частей подлинных купюр, наклейки частей подлинных купюр со средствами защиты на листы бумаги или сувенирные купюры). Схема преступной деятельности такова: злоумышленник, используя банковскую карту, производит через банкомат операцию пополнения банковского счета наличными денежными средствами, вставляет поддельную (сувенирную) денежную купюру в купюроприемник банкомата, банкомат распознает ее как подлинную, в результате чего банковская компьютерная система зачисляет денежные средства на банковский счет виновного [13, с. 79–83; 14, с. 46–50].

Хищение денежных средств банка в указанных случаях происходит под воздействием обманных манипуляций, однако теоретики не усматривают здесь наличия состава мошенничества, ссылаясь на невозможность обмана компьютерной системы банкомата [15, с. 48–58]. Судебная практика в целом разделяет этот подход, хотя некоторые суды все же вменяют мошенничество путем обмана банка[7].

Обманное воздействие на компьютерную систему используется также для хищений денежных средств банков путем имитации внесения наличных денежных средств на банковский счет посредством банкомата. Подобные хищения совершаются по следующей схеме: злоумышленник с использованием банковской карты инициирует в банкомате операцию по внесению наличных денежных средств на расчетный счет, к которому привязана карта, но денежные средства фактически не вносит, удерживая при этом шторку купюроприемника; эти действия вызывают аппаратный сбой в работе банкомата — на его экране появляется сообщение об ошибке с предложением указать сумму денежных средств, внесенных клиентом, но не зачисленных вследствие сбоя в работе банкомата; субъект вводит заведомо ложную информацию о внесении денежных средств; эта информация обрабатывается компьютерной системой банка, которая в автономном режиме (без участия сотрудника банка) принимает решение о зачислении денежных средств на банковский счет платежной карты, при условии, что сумма денежных средств не превышает определенного предела (как правило, не более 5 000 р.) (в случае превышения этой суммы зачисление денежных средств на счет клиента происходит только после его обращения в офис банка).

Несмотря на то, что указанные деяния основаны на обмане, в уголовно-правовой доктрине отмечается невозможность их квалификации по ст. 159 УК РФ. Довод тот же самый — воздействие на психику человека в рассматриваемых ситуациях не осуществляется, а значит, мошеннического обмана здесь нет. Следуя этой парадигме, сформировавшейся в XIX столетии, представители уголовно-правовой науки обосновывают стандартный дифференцированный подход к уголовно-правовой оценке хищений, совершаемых путем имитации внесения налич-

[6] В правоприменительной практике потерпевшим от преступления в рассматриваемых случаях нередко признается физическое лицо, от имени которого злоумышленник подавал заявку на получение кредита. Соответственно, получение кредита на это физическое лицо расценивается в качестве приготовления к последующему хищению денежных средств с банковского счета физического лица. Однако такой подход представляется ошибочным, на что справедливо обращается внимание в доктрине [11, с. 15–19].

[7] См., например: постановление Первореченского районного суда города Владивостока от 19.12.2019 по делу № 1-24/2019.

ных денежных средств на банковский счет посредством банкомата: при введении заведомо ложной информации в компьютерную систему банка хищение предлагается считать тайным, а при обмане сотрудника банка рекомендуется вменять мошенничество [15, с. 48–58].

В результате практического применения этих доктринальных рекомендаций возникает парадоксальная (если не сказать абсурдная) ситуация: хищение на небольшую сумму (не более 5 000 рублей), совершенное путем ввода в компьютерную систему банка заведомо ложной информации о якобы внесенных наличных денежных средствах, признается тяжким преступлением — кражей с банковского счета (п. «г» ч. 3 ст. 158 УК РФ), тогда как хищение в размере до 250 000 рублей, совершенное путем сообщения той же недостоверной информации сотруднику банка, расценивается как преступление небольшой тяжести — простое мошенничество (ч. 1 ст. 159 УК РФ).

Таким образом, консервативные представления о мошенническом обмане, зафиксированные в п. 1 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48, порождают «перекосы» в правоприменительной практике, несовместимые с принципами уголовного права, конституционными императивами и элементарным здравым смыслом. Приходится признать, что современное уголовное право России не способно обеспечить адекватную квалификацию хищений, совершаемых путем обманного воздействия на компьютерную систему.

5. В поиске решения обозначенной проблемы, которая имеет интернациональный характер и не знает государственных границ, целесообразно обратиться к зарубежному опыту. В зарубежных правопорядках используются два основных подхода к уголовно-правовому противодействию хищениям, совершаемым посредством «обмана» компьютерной системы.

Первый из них предполагает конструирование самостоятельных уголовно-правовых норм об ответственности за хищения путем воздействия на компьютерную систему, что позволяет сохранить традиционную трактовку мошеннического обмана как воздействия на психику человека. Именно по такому пути пошел немецкий законодатель, включив в УК ФРГ §263а «Компьютерное мошенничество». На основании §263а УК ФРГ наказывается тот, «кто умышленно или с намерением создать для себя или третьего лица противоправную имущественную выгоду наносит ущерб другому лицу таким образом, что влияет на результат обработки данных путем создания неправильных программ, использования неправильных или неполных данных, неправомочным использованием данных или иным образом неправомерно воздействуя на данный процесс».

В немецкой уголовно-правовой доктрине отмечается, что в отличие от общей нормы о мошенничестве (§ 263 УК ФРГ) при совершении компьютерного мошенничества (§ 263а УК ФРГ) отсутствует живой человек, совершающий под влиянием обмана сделку с имуществом, а имеются лишь определенные манипуляции с системой обработки компьютерной информации (Datenverarbeitungssystem) [16–19, с. 463; 20, с. 55–59]. При этом обман как способ «классического» мошенничества (§263 УК ФРГ) понимается традиционно как воздействие на психику человека: «Последствием обмана должно стать *заблуждение (Irrtum)* человека относительно фактов, обман либо вводит человека в заблуждение, либо поддерживает в нем заблуждение, возникшее раньше. Манипулирование машинами и компьютерными системами не образует мошенничества, в этом случае содеянное может быть квалифицировано как компьютерное мошенничество (§ 263а StGB)» [21, с. 186].

Таким образом, норму об ответственности за компьютерное мошенничество (§ 263а УК ФРГ), несмотря на ее наименование, нельзя считать специальной по отношению к норме об ответственности за мошенничество (§ 263а УК ФРГ), ведь «она применяется при отсутствии признаков мошенничества» [21, с. 189]. Эта норма позволила восполнить недостаточность уголовного закона, сохранив в неприкосновенности традиционное содержание нормы об ответственности за мошенничество и устоявшуюся интерпретацию мошеннического обмана.

Второй подход заключается в существенном расширении содержания мошеннического обмана, позволяющем распространить его на ввод заведомо ложной информации в компьютерную систему. В частности, такое решение реализовано в Великобритании в Акте о мошенничестве 2006 г.[8] Раздел 2 Акта о мошенничестве одной из форм мошенничества признает «мошенничество путем ложного представления»,

[8] URL: https://www.cps.gov.uk/legal-guidance/fraud-act-2006 (дата обращения: 03.02.2025).

которое констатируется при условии, что субъект «сделал ложное заявление нечестно, зная, что заявление было или может быть неверным или вводящим в заблуждение, с намерением получить выгоду для себя или другого лица, причинить убытки другому лицу или подвергнуть другое лицо риску убытков». При этом заявлением признается любое утверждение, относящееся к факту или закону, переданное в любой форме человеку или на устройство, предназначенное для обработки информации [22, p. 524–553]. Комментируя положения разд. 2 Акта о мошенничестве, И.А. Клепицкий пишет: «Преступление окончено, когда представление (или нечто, его подразумевающее) сделано не только человеку, но и в любой форме передано любой системе или устройству, предназначенному для приема, передачи или ответа на сообщения (в том числе и без вмешательства человека)» [21, с. 137]. Таким образом, в Великобритании широкая трактовка мошеннического обмана охватывает не только обманное воздействие на психику человека, но и ввод заведомо ложной информации в компьютерную систему.

6. Адаптируя уголовный закон для противодействия цифровой преступности, в 2012 г. отечественный законодатель в рамках масштабного реформирования гл. 21 УК РФ попытался создать аналог немецкой уголовно-правовой нормы об ответственности за компьютерное мошенничество (§263а УК ФРГ). Федеральным законом от 29.11.2012 № 207-ФЗ в гл. 21 УК РФ включено шесть новых статей, в том числе ст. 159.6 об ответственности за мошенничество в сфере компьютерной информации. В пояснительной записке к соответствующему законопроекту отмечалась архаичность ст. 159 УК РФ, которая фактически воспроизводит аналогичную норму УК РСФСР, обращалось внимание на необходимость разработки адекватных уголовно-правовых мер воздействия на новые схемы хищений и незаконного приобретения права на него. Обосновывая потребность в конструировании ст. 159.6 УК РФ, разработчики законопроекта особо оговаривали, что преступления, предусмотренные проектируемой статьей, «совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий (перечисленных в диспозиции ст. 159.6 УК РФ. — *К.О.)*, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество»[9]. Таким образом, в плане концептуальной законодательной идеи параллели ст. 159.6 УК РФ с § 263а УК ФРГ об ответственности за компьютерное мошенничество вполне очевидны.

Правда, в результате заимствования немецкого законодательного опыта на российскую нормативную «почву» были перенесены не только несомненные достоинства § 263а УК ФРГ, но и ее недостатки, а именно — неудачное название нормы, построенное на базе термина «мошенничество». Основное предназначение § 263а УК ФРГ и ст. 159.6 УК РФ заключается в том, чтобы создать нормативную основу для квалификации хищений, совершаемых путем воздействия на компьютерную информацию и (или) компьютерные системы, и тем самым выйти за пределы узкой сферы применения «классических» норм об ответственности за мошенничество путем обмана человека (§ 263 УК ФРГ и ст. 159 УК РФ). Поэтому термин «мошенничество» в этих статьях неуместен; он лишь вводит в заблуждение[10].

Тем не менее главная проблема была решена: не меняя привычной трактовки мошеннического обмана, законодатель сконструировал норму, позволяющую квалифицировать хищения, совершаемые путем воздействия (в том числе обманного) на компьютерную систему. В 2013–2017 гг. ст. 159.6 УК РФ довольно активно применялась для квалификации хищений, совершенных путем введения заведомо ложных данных в компьютерные системы[11]. В частности, по ст. 159.6 УК РФ квалифицировались хищения безналичных денежных средств, совершаемые: посредством авторизации в банковском приложении под чужим именем (с использованием учетных данных владельца банковского счета) и перевода денежных средств, размещенных на банковском счете потерпевшего, на банковский счет виновного (иной подконтрольный ему счет); путем направления с чужого телефона СМС-сообщения на номер 900, т.е. подачи элек-

[9] Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».

[10] В доктрине справедливо отмечается, что в ст. 159.6 УК РФ предусмотрена самостоятельная форма хищения, отличная от мошенничества [23, с. 35–36; 24, с. 132; 25, с. 598–609].

[11] Обзор соответствующей судебной практики представлен в следующих работах: [26, с. 12–16; 27, с. 36–43; 28, с. 92–97; 29, с. 229–234].

тронного распоряжения банку о перечислении денежных средств со счета потерпевшего на свой банковский счет; посредством внесения в банкомат частей подлинных денежных купюр[12].

Отграничение мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) от «классического» мошенничества (ст. 159 УК РФ) осуществлялось с учетом традиционных представлений об обмане: ст. 159.6 УК РФ применялась только в тех случаях, когда хищение совершалось посредством воздействия на компьютерную информацию, не связанном с обманом человека; при обмане человека хищение квалифицировалось по ст. 159 УК РФ, даже если обман был облечен в «цифровую» форму [30, с. 43]. Таким образом, главным критерием разграничения указанных преступлений выступал не способ предоставления заведомо ложной информации («аналоговый» или «цифровой»), а ее адресат (человек или машина).

7. Однако через пять лет после введения ст. 159.6 УК РФ из сферы ее применения были исключены хищения, совершаемые путем ввода заведомо ложной информации в компьютерную систему. В п. 20 постановления Пленума от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей предписано понимать «целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры)… или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации…». При этом в п. 21 цитируемого постановления Пленума разъяснено, что «в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным …, такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети».

Таким образом, в результате ограничительного толкования способов, указанных в ст. 159.6 УК РФ, эта норма применяется только в тех случаях, когда хищение совершено посредством «взлома» компьютерной системы, т.е. путем внештатного воздействия на нее, не предусмотренного разработчиками [31, с. 213]. Хищение путем ввода в компьютерную систему заведомо ложной информации (например, авторизация в системе дистанционного банковского обслуживания с использованием чужих учетных данных, ввод команды о перечислении денежных средств от имени другого лица, подписание электронного договора без намерения выполнять принятые обязательства) квалифицируется теперь как банальная кража. И это при том, что в ч. 1 ст. 159.6 УК РФ в качестве способа совершения преступления прямо указан ввод компьютерной информации.

В итоге ст. 159.6 УК РФ, специально сконструированная для противодействия хищениям, совершаемым путем воздействия на компьютерную систему, свое предназначение не выполняет: в 2023 г. по этой статье осуждено 15 чел., тогда как в 2017 г. этот показатель был на порядок выше (144 осужденных). Высший судебный орган приспособил для квалификации подобных деяний архаичную ст. 158 УК РФ, полностью перечеркнув концепцию своей же законодательной инициативы (напомним, что разработчиком законопроекта, предполагающего дифференциацию ответственности за мошенничество за счет специальных норм, выступал именно Верховный Суд).

Результаты известны: сходные по сути обманные схемы хищения получают различную квалификацию в зависимости от способа обработки ложных данных, предоставленных похитителем, причем «цена» дифференцированной уголовно-правовой оценки исчисляется годами лишения свободы.

8. Тем не менее здравый смысл и каноны справедливости оказываются сильнее доктринальных догматов и разъяснений Пленума Верховного Суда. В стремлении обеспечить адекватную уголовно-правовую оценку анализируемых видов хищений, суды, лишенные возможности

[12] В работах, опубликованных до принятия постановления Пленума от 30.11.2017 № 48, отмечалось, что эти действия следует квалифицировать по ст. 159.6 УК РФ, поскольку «все иные нормы, устанавливающие уголовную ответственность за мошенничество, предполагают, что хищение чужого имущества совершается посредством обмана человека, и только ст. 159.6 УК РФ предусматривает в качестве способа совершения преступления, если так можно выразиться, «обман» электронно-вычислительной машины или компьютерной программы» [13, с. 79–83].

применять ст. 159.6 УК РФ, все чаще приравнивают обманное воздействие на компьютерную систему к обману человека.

Показательным в этом отношении можно считать решение Четвертого кассационного суда общей юрисдикции. Соглашаясь с квалификацией действий осужденного А. по ч. 3 ст. 159 УК РФ, суд кассационной инстанции указал следующее: «Несмотря на то, что кредиты были предоставлены банком по заявкам, проверенным банковской программой без участия сотрудников банка, обман, как способ совершения преступления имеет место, поскольку банковская программа в любом случае контролируется сотрудниками банка и в данном случае выступает в качестве способа доведения до банка не соответствующих действительности сведений о том, что за получением кредитов обращался ФИО10. Перекладывая на банковскую программу функции по обработке заявок, заключению договоров и выдаче кредитов банк тем самым опосредовал при ее помощи интеллектуальную составляющую волевого момента при заключении договоров и выдаче кредитов. В этой связи *предоставление посредством банковской программы банку не соответствующих действительности сведений влечет за собой не обман самой программы* (здесь и далее курсив мой. — *О. В.)*, как об этом указывает автор кассационной жалобы, *а непосредственно банка*»[13]. Аналогичное решение со сходной аргументацией принято Восьмым кассационным судом общей юрисдикции[14]. Таким образом, кассационные суды расценили дистанционное внесение ложных данных в электронную заявку на получение кредита как опосредованный обман банка, и на этом основании квалифицировали хищение по ст. 159 УК РФ.

Руководствуясь той же логикой, Второй кассационный суд общей юрисдикции квалифицировал хищение денежных средств банка путем имитации внесения наличных денежных средств на банковский счет с использованием банкомата по ст. 159.3 УК РФ, несмотря на то, что обработка заведомо ложных сведений и принятие решения о зачислении денежных средств осуществлялись компьютерной программой без участия человека. В обоснование принятого решения суд кассационной инстанции указал следующее: «…в банке существовала подача претензий на сумму до 5 000 рублей в автоматическом режиме, то есть без участия сотрудников банка по упрощенной системе урегулирования. *Внося заведомо ложные сведения о техническом сбое операционной системы банкомата в претензию, направленную через удаленные каналы обслуживания банка, Г., по сути, обманывал банк*. … При этом диспозиция ни ч. 1 ст. 159 УК РФ, ни ч. 1 ст. 159.3 УК РФ не содержит обязательного условия обмана непосредственно конкретного физического лица». Еще одним и, пожалуй, главным доводом в пользу квалификации по ст. 159.3 УК РФ стал принцип справедливости (в его широком понимании): «…судебная коллегия констатирует, что при одномоментном хищении таким способом чужого имущества на сумму свыше 5 000 рублей виновный должен был непосредственно явиться в офис банка и сообщить заведомо ложные сведения о техническом сбое в работе операционной системы банкомата одному из сотрудников. В этом случае его действия должны быть квалифицированы как мошенничество. Тем самым квалификация содеянного, как кража или мошенничество, зависела бы от размера похищенного, что противоречило бы уголовно-правовому принципу назначения более строгого наказания за более тяжкое преступление. При таких обстоятельствах судебная коллегия не находит оснований и для переквалификации действий Г. на ч. 1 ст. 158 УК РФ, о чем ставится вопрос в кассационной жалобе. Таким образом, действия Г. подлежат переквалификации на ч. 1 ст. 159.3 УК РФ, поскольку при хищении он использовал электронные средства платежа, которые впоследствии обналичивал»[15].

Следует отметить, что конструкция обвинения в мошенничестве, основанная на опосредованном обмане юридического лица (государственного органа), довольно часто встречается в правоприменительной практике. И хотя такую конструкцию нельзя признать теоретически безупречной с позиции традиционного понимания обмана (если введен в заблуждение сотрудник

[13] Кассационное определение Четвертого кассационного суда общей юрисдикции от 24.05.2022 № 77-2141/2022.

[14] Определение Восьмого кассационного суда общей юрисдикции от 20.12.2023 № 77-5359/2023.

[15] Кассационное определение Второго кассационного суда общей юрисдикции от 01.04.2022 № 77-991/2022. Аналогичные решения см.: определение Шестого кассационного суда общей юрисдикции от 17.09.2024 № 77-3300/2024; апелляционное определение Белгородского областного суда от 20.06.2022 по делу № 22-836/2022; апелляционное определение Воронежского областного суда от 27.10.2022 № 22-2824/2022.

организации или государственного органа, то в обвинении, по идее, необходимо ссылаться на обман этого сотрудника, а не юридического лица в целом), высшие суды не усматривают в ней особой «крамолы»: «Довод кассационной жалобы о том, что обман, как способ совершения мошенничества не может быть использован в отношении юридического лица, основан на неверном толковании уголовного закона, поскольку диспозиция ст. 159 УК РФ не содержит в качестве обязательного признака состава преступления — совершение преступления в отношении физического лица»[16]. Более того, возможность мошеннического обмана юридического лица (в частности, кредитной организации) допускает и Конституционный Суд Российской Федерации[17].

Такая практика пока не стала общепризнанной, но тренд, полагаю, очевиден. Наблюдается отход от классических представлений о мошенническом обмане (причем не только на уровне правоприменения, но и в доктрине [32]): его адресатом признается уже не только человек, но и юридическое лицо. Причем эта юридическая конструкция (обман юридического лица), воспринятая практикой, позволяет признавать мошенническим обманом ввод заведомо ложной информации в компьютерную систему: надо лишь только сослаться на обман организации, не употребляя табуированное словосочетание «обман компьютерной системы».

Похоже на то, что после резкого ограничения сферы применения ст. 159.6 УК РФ, состоявшегося в 2017 г., правоприменительная практика постепенно разворачивается в сторону широкой трактовки мошеннического обмана, подобной той, что используется в британском Акте о мошенничестве 2006 г. По мере распространения хищений, реализуемых посредством ввода ложной информации в компьютерную систему, становится все более очевидным, что норма об ответственности за кражу плохо приспособлена для квалификации подобных деяний. Квалификация по п. «г» ч. 3 ст. 158 УК РФ не отражает сущности этих преступных деяний, основанных на обмане, что вынуждает правоприменителей «подводить» их под ст. 159 УК РФ за счет расширительного толкования обмана.

9. Остановить эрозию классических представлений о мошенническом обмане можно только в том случае, если субъекты правоприменения получат адекватный уголовно-правовой инструментарий для юридической оценки рассматриваемых деяний. Конструировать для этого новую уголовно-правовую норму необязательно, достаточно скорректировать ст. 159.6 УК РФ:

– исключить из нее упоминание о мошенничестве, изложив название статьи в следующем виде: «Хищение путем ввода компьютерной информации или вмешательства в функционирование компьютерного устройства»;

– в качестве способов совершения преступления альтернативно регламентировать следующие неправомерные действия: ввод в компьютерное устройство команд от имени другого лица; ввод в компьютерное устройство заведомо ложной информации; вмешательство в функционирование компьютерного устройства или информационно-телекоммуникационной сети;

– исключить из ч. 3 ст. 159.6 УК РФ квалифицирующий признак «с банковского счета, а равно в отношении электронных денежных средств», а также уравнять санкции ч. 1–4 ст. 159.6 УК РФ с санкциями ч. 1–4 ст. 159 УК РФ, что позволит устранить диспропорции в уголовно-правовом реагировании на мошеннический обман человека и обманное воздействие на компьютерную систему.

В технико-юридическом смысле предложенный вариант реформирования ст. 159.6 УК РФ может потребовать (и наверняка потребует) доработки, но его концепция, надеюсь, вполне понятна. В таком виде ст. 159.6 УК РФ будет охватывать хищения и факты противоправного приобретения права на имущество, которые совершаются не только путем «взлома» компьютерной системы, но и посредством обманного воздействия на нее, не нарушающего штатные процессы ее функционирования. Предвидя возможные возражения, связанные с различиями в степени общественной опасности указанных способов хищения (понятно, что хакерский «взлом» компьютерного устройства или программы более опасен, чем простой ввод команды на перевод денежных средств), поясним, что дифференциация уголовной ответственности будет осуществляться за счет дополнительной

[16] Определение Первого кассационного суда общей юрисдикции от 29.04.2021 № 77-1186/2021. Аналогичная позиция отражена и в иных решениях судов кассационной и апелляционной инстанции (см.: кассационное определение Второго кассационного суда общей юрисдикции от 01.04.2022 № 77-991/2022; апелляционное определение Свердловского областного суда от 26.06.2018 по делу № 22-3716/2018 и др.).

[17] Определение Конституционного Суда Российской Федерации от 09.07.2021 № 1374-О (абз. 6 п. 5.1).

квалификации: «взлом» компьютерного устройства с использованием вредоносных компьютерных программ потребует дополнительного вменения ст. 273 УК РФ, тогда как при совершении хищения путем ввода в компьютерное устройство заведомо ложной информации или команд от имени другого лица ст. 273 УК РФ применяться не будет.

Практическая реализация изложенных инициатив позволит создать нормативную основу для уголовно-правового противодействия хищениям, совершаемым путем обманного воздействия на компьютерную систему, сохранив при этом устоявшуюся трактовку мошеннического обмана. Причем откладывать принятие соответствующих законодательных решений нельзя, ведь стремительное развитие технологий искусственного интеллекта и их активное внедрение в экономику и управление (причем не только в коммерческом, но и в государственном секторе) позволяет с уверенностью прогнозировать, что обманное воздействие на компьютерные системы банков, электронных торговых площадок, налоговых и иных государственных органов довольно скоро встанет в один ряд с наиболее распространенными способами хищений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Клепицкий И. Мошенничество и правонарушения гражданско-правового характера / И. Клепицкий. — EDN IIDQVS // Законность. — 1995. — № 7. — С. 41–43.

2. Лопашенко Н.А. Преступления против собственности. Авторский курс : в 4 кн. / Н.А. Лопашенко. — Москва : Юрлитинформ, 2019. — Кн. 3. Формы хищения. — 264 с.

3. Хилюта В.В. Хищение: системный кризис института и проблемы квалификации : монография / В.В. Хилюта. — Москва : Юрлитинформ, 2021. — 422 с.

4. Архипов А.В. Законодательство об уголовной ответственности за хищения в России: проблемы правоприменения и концептуальные основы реформирования : монография / А.В. Архипов. — Москва : Юрлитинформ, 2022. — 311 с.

5. Яни П.С. Постановление Пленума Верховного Суда о квалификации мошенничества, присвоения и растраты: проблемы разграничения и совокупности / П.С. Яни. — EDN LETRET // Законность. — 2008. — № 6. — С. 12–16.

6. Шипунова М.Н. «Обман» компьютерной системы как способ совершения преступления / М.Н. Шипунова. — EDN TEQLSD // Уголовная политика в условиях цифровой трансформации : материалы II Всерос. науч.-практ. конф., Казань, 27 апр. 2023 г. — Казань, 2023. — С. 47–52.

7. Петров С.А. Проблемы квалификации хищений при кредитном скоринге / С.А. Петров. — EDN BNOTQO // Законность. — 2019. — № 6. — С. 47–51.

8. Городецкая О.Ю. Ключевые тренды применения искусственного интеллекта в банковской сфере / О.Ю. Городецкая, Я.Л. Гобарева. — EDN TZIWZV // Финансовые рынки и банки. — 2022. — № 12. — С. 34–42.

9. Смирнов Е. Скоринг за секунды: как нейросети изменили выдачу кредитов / Е. Смирнов // РБК. — URL: https://trends.rbc.ru/trends/industry/cmrm/644942449a7947981d14f327?from=copy.

10. Царев К. 99 % решений по кредитам в Сбере принимает искусственный интеллект / К. Царев // РБК. — URL: https://plus.rbc.ru/news/638ceb2a7a8aa97b488a6194.

11. Архипов А.В. Квалификация хищения путем дистанционного оформления кредита от чужого имени / А.В. Архипов. — DOI 10.52390/20715870_2023_3_15. — EDN HVZRIF // Уголовное право. — 2023. — № 3. — С. 15–19.

12. Быкова Е.Г. Сложности квалификации хищения с банковского счета при дистанционном оформлении кредита от имени его владельца / Е.Г. Быкова. — DOI 10.52390/20715870_2022_7_3. — EDN JLQKYX // Уголовное право. — 2022. — № 7.

13. Прозументов Л.М. Квалификация сбыта поддельных банкнот посредством банкоматов / Л.М. Прозументов, А.В. Архипов. — EDN WHWTJF // Уголовное право. — 2016. — № 2. — С. 79–83.

14. Турышев А.А. Квалификация хищения с использованием банкоматов / А.А. Турышев. — EDN VZVMUP // Законы России: опыт, анализ, практика. — 2016. — № 6. — С. 46–49.

15. Скляров С.В. Квалификация хищения с использованием платежной карты путем имитации внесения наличных денежных средств на банковский счет посредством банкомата / С.В. Скляров. — DOI 10.52390/20715870_2023_11_48. — EDN ONYVHK // Уголовное право. — 2023. — № 11. — С. 48–58.

16. Fischer T. Strafgesetzbuch / T. Fischer. — 61. Auflage. — Verlag C.H. Beck, 2014. — 2685 p.

17. Lackner K. Strafgesetzbuch / K. Lackner, K. Kühl. — 27. Auflage, 2011. — 1660 p.

18. Systematischer Kommentar zum Strafgesetzbuchh / H.-J. Rudolphi, E. Horn, E. Samson [et al.]. — 4. Auflage. — Baden-Baden : Nomos Verlagsgesellschaft, 2013.

19. Жалинский А.Э. Современное немецкое уголовное право / А.Э. Жалинский. — Москва : Проспект, 2006. — 560 с.

20. Харламов Д.Д. Уголовная ответственность за компьютерное мошенничество по УК российской Федерации и ФРГ / Д.Д. Харламов. — EDN UFGIOB // Бизнес в законе. — 2015. — № 4. — С. 55–59.

21. Клепицкий И.А. Новое экономическое уголовное право : монография / И.А. Клепицкий. — Москва : Проспект, 2021. — 983 с.

22. Herring Jonatan. Criminal Law: Text, Cases, and Materials / Herring Jonatan. — Oxford, 2012. — 999 p.

23. Яни П.С. Специальные виды мошенничества / П.С. Яни. — EDN UHLBGJ // Законность. — 2015. — № 8. — С. 35–40.

24. Чупрова А.Ю. Проблемы квалификации мошенничества с использованием информационных технологий / А.Ю. Чупрова. — EDN: UNXAOJ // Уголовное право. — 2015. — № 5. — С. 131–134.

25. Лопашенко Н.А. Компьютерное мошенничество — новое слово в понимании хищения или ошибка законодателя? / Н.А. Лопашенко. — EDN CIQENR // Пермский юридический альманах. — 2019. — № 2. — С. 598–609.

26. Болсуновская Л. Мошенничество в сфере компьютерной информации: анализ судебной практики / Л. Болсуновская. — EDN WHWTEZ // Уголовное право. — 2016. — № 2. — С. 12–16.

27. Ермакова О.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): сложности толкования и квалификации / О.В. Ермакова. — EDN WHWTPT // Уголовное право. — 2016. — № 3. — 36–43.

28. Тюнин В.И. Мошенничество в сфере компьютерной информации: сложности квалификации / В.И. Тюнин. — EDN YQNPKP // Уголовное право. — 2017. — № 5. — С. 92–97.

29. Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / С.В. Шевелева. — EDN ZXRFXL // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2017. — № 4. — С. 229–234.

30. Третьяк М. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М. Третьяк. — EDN WMWMFB // Законность. — 2016. — № 7. — С. 41–46.

31. Архипов А.В. Квалификация мошенничества по уголовному законодательству России : монография / А.В. Архипов; под ред. Л.М. Прозументова. — Москва : Юрлитинформ, 2020. — 232 с. — EDN UIQYXT.

32. Яни П.С. Вопросы квалификации мошеннического обмана суда / П.С. Яни. — EDN HLTZVD // Законность. — 2024. — № 1. — С. 26–30.

REFERENCES

1. Klepitskii I. Fraud and Offences of Civil Law Character. *Zakonnost = Legality*, 1995, no. 7, pp. 41–43. (In Russian). EDN: IIDQVS.

2. Lopashenko N.A. *Crimes against Property.* Moscow, Yurlitinform Publ., 2019. Bk. 3. 264 p.

3. Khilyuta V.V. *Theft: A Systemic Crisis of the Institute and the Problems of Qualification.* Moscow, Yurlitinform Publ., 2021. 422 p.

4. Arkhipov A.V. *Legislative Regulation of Criminal Liability for Theft in Russia: Problems of Law Enforcement and the Conceptual Basis of Reforms.* Moscow, Yurlitinform Publ., 2022. 311 p.

5. Yani P.S. Decree of the Plenary Session of the Supreme Court on the Qualification of Fraud, Appropriation and Embezzlement: Problems of Delineation and Accumulation. *Zakonnost = Legality*, 2008, no. 6, pp. 12–16. (In Russian). EDN: LETRET.

6. Shipunova M.N. «Deception» of a Computer System as a Way to Commit a Crime. *Criminal Policy in the Conditions of Digital Transformation. Materials of International Scientific Conference, Kazan, April 27, 2023.* Kazan', 2023, pp. 47–52. (In Russian). EDN: TEQLSD.

7. Petrov S.A. The Problems of Classification of Thefts in Loan Scoring. *Zakonnost' = Legality*, 2019, no. 6, pp. 47–51. (In Russian). EDN: BNOTQO.

8. Gorodetskaya O.Yu., Gobareva Ya.L. Key Trends in the Application of Artificial Intelligence in the Banking Sector. *Finansovye rynki i banki = Financial Markets*, 2022, no. 12, pp. 34–42. (In Russian). EDN: TZIWZV.

9. Smirnov E. Scoring within Seconds: How Neural Networks Changed Issuing Loans. *RBK*. URL: https://trends.rbc.ru/trends/industry/cmrm/644942449a7947981d14f327?from=copy. (In Russian).

10. Tsarev K. 99% of Decisions on Loans in Sberbank are Made by Artificial Intelligence. *RBK*. URL: https://plus.rbc.ru/news/638ceb2a7a8aa97b488a6194. (In Russian).

11. Arkhipov A.V. Qualification of Misappropriation Through Remote Loan Processing on Behalf of Others. *Ugolovnoe pravo = Criminal Law*, 2023, no. 3, pp. 15–19. (In Russian). EDN: HVZRIF. DOI: 10.52390/20715870_2023_3_15.

12. Bykova E.G. Difficulties in the Qualification of Misappropriation from a Bank Account in Remote Loan Arrangement on Behalf of its Owner. *Ugolovnoe pravo = Criminal Law*, 2022, no. 7, pp. 3–13. (In Russian). EDN: JLQKYX. DOI: 10.52390/20715870_2022_7_3.

13. Prozumentov L.M., Arkhipov A.V. Classification of Sale of Counterfeit Banknotes Through ATM Machines. *Ugolovnoe pravo = Criminal Law,* 2016, no. 6, pp. 79–83. (In Russian). EDN: WHWTJF.

14. Turyshev A.A. Qualifications of Misappropriation with Using Atms. *Zakony Rossii: opyt, analiz, praktika = Law of Russia: Experience, Analysis, Practice*, 2016, no. 6, pp. 46–49. (In Russian). EDN: VZVMUP.

15. Sklyarov S.V. Qualification of Card-related Theft by Imitation of Cash Deposit to a Bank Account Through an ATM. *Ugolovnoe pravo = Criminal Law*, 2023, no. 11, pp. 48–58. (In Russian). EDN: ONYVHK. DOI: 10.52390/20715870_2023_11_48.

16. Fischer T. *Strafgesetzbuch*. 61. Auflage. Verlag C.H. Beck, 2014. 2685 p.

17. Lackner K., Kühl K. *Strafgesetzbuch*. 27. Auflage, 2011. 1660 p.

18. Rudolphi H.-J., Horn E., Samson E., Günther H.-L., Hoyer A. *Systematischer Kommentar zum Strafgesetzbuchh*. 4. Auflage Baden-Baden, Nomos Verlagsgesellschaft, 2013.

19. Zhalinskii A.Eh. *Modern German Criminal Law.* Moscow, Prospekt Publ., 2006. 560 p.

20. Kharlamov D.D. The Criminal Liability for Computer Fraud According to Russian and German Criminal Code. *Biznes v zakone = Business in Law*, 2015, no. 4, pp. 55–59. (In Russian). EDN: UFGIOB.

21. Klepitskii I.A. *New Economic Criminal Law.* Moscow, Prospekt Publ., 2021. 983 p.

22. Herring Jonatan. *Criminal Law: Text, Cases, and Materials*. Oxford, 2012. 999 p.

23. Yani P.S. Specific Types of Fraud. *Zakonnost = Legality*, 2015, no. 8, pp. 35–40. (In Russian). EDN: UHLBGJ.

24. Chuprova A.Yu. The Problems of Classification of Fraud Related to Use of Information Technologies. *Ugolovnoe pravo = Criminal Law*, 2015, no. 5, pp. 131–134. (In Russian). EDN: UNXAOJ.

25. Lopashenko N.A. Cybercrime: Advance in the Understanding of Fraud or a Lawmaker's Mistake? *Permskij juridicheskij al'manah = Perm Legal Almanac*, 2019, no. 2, pp. 598–609. (In Russian). EDN: CIQENR.

26. Bolsunovskaya L. IT Crime: Court Case Law Analysis. *Ugolovnoe pravo = Criminal Law*, 2016, no. 2, pp. 12–16. (In Russian). EDN: WHWTEZ.

27. Ermakova O.V. Computer Fraud (Article 1596 of the Criminal Code of the Russian Federation): Difficulties of Interpretation and Classification. *Ugolovnoe pravo = Criminal Law*, 2016, no. 3, pp. 36–43. (In Russian). EDN: WHWTPT.

28. Tyunin V.I. Fraud in the Sphere of Computer Information: Difficulties of Classification. *Ugolovnoe pravo = Criminal Law*, 2017, no. 5, pp. 92–97. (In Russian). EDN: YQNPKP.

29. Sheveleva S.V. Fraud in the Sphere of Computer Information: Specifics of Qualification and Competition with Related Offences. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice: Journal of Nizhniy Novgorod Academy of the Ministry of the Interior of the Russian Federation*, 2017, no. 4, pp. 229–234. (In Russian). EDN: ZXRFXL.

30. Tret'yak M. The Problem of Legal Regulation of Hi-Tech Property Crimes. *Zakonnost = Legality*, 2016, no. 7, pp. 41–46. (In Russian). EDN: WMWMFB.

31. Arkhipov A.V.; Prozumentov L.M. (ed.). *Qualification of Fraud under Russian Criminal Legislation.* Moscow, Yurlitinform Publ., 2020. 232 p. EDN: UIQYXT.

32. Yani P.S. Issues of Qualification of Fraudulent Deception of the Court. *Zakonnost = Legality*, 2024, no. 1, no. 1, pp. 26–30. (In Russian). EDN: HLTZVD.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ображиев Константин Викторович — профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: okv79@mail.ru, https://orcid.org/0009-0003-8399-3799.

ДЛЯ ЦИТИРОВАНИЯ

Ображиев К.В. Обманное воздействие на компьютерную систему как способ хищения / К.В. Ображиев. — DOI 10.17150/2500-4255.2025.19(2).160-172. — EDN DLNAFD // Всероссийский криминологический журнал. — 2025. — Т. 19, № 2. — С. 160–172.

INFORMATION ABOUT THE AUTHOR

Obrazhiev, Konstantin V. — Professor, Department of Criminal Law, Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: okv79@mail.ru, https://orcid.org/0009-0003-8399-3799.

FOR CITATION

Obrazhiev K.V. Fraudulent Influence on a Computer System as a Method of Theft. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2025, vol. 19, no. 2, pp. 160–172. (In Russian). EDN: DLNAFD. DOI: 10.17150/2500-4255.2025.19(2).160-172.