Юридические исследования
*Правильная ссылка на статью:*
Полстовалов О.В., Галяутдинов Р.Р. — Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения // Юридические исследования. – 2023. – № 11. DOI: 10.25136/2409-7136.2023.11.44223 EDN: MXFWZI URL: https://nbpublish.com/library_read_article.php?id=44223

# Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения

**Полстовалов Олег Владимирович**

ORCID: 0000-0003-4991-990X

доктор юридических наук

профессор кафедры криминалистики, Институт права, Уфимский университет науки и технологий"

450077, Россия, республика Башкортостан, г. Уфа, ул. Достоевского, 131

kriminalist2010@mail.ru

**Галяутдинов Рушан Радикович**

ORCID: 0000-0002-1205-7608

кандидат юридических наук

доцент, кафедра криминалистики, Институт права ФГБОУ ВО "Уфимский университет науки и технологий"

450077, Россия, республика Башкортостан, г. Уфа, ул. Достоевского, 131

rushan-94@mail.ru

Статья из рубрики "Уголовный закон и правопорядок "

**DOI:**

10.25136/2409-7136.2023.11.44223

**EDN:**

MXFWZI

**Дата направления статьи в редакцию:**

05-10-2023

**Аннотация:** Актуальность темы исследования. Правоохранительная и судебная практика в России столкнулась с массой ранее не существовавших видов мошенничества. Так

появилось мошенничество в сфере компьютерной технологии и использования высоких технологий. Наряду с этим развитие секторов экономики, кредитно-финансовой системы, коммерческих банков, появление новых информационных, банковских технологий, технических средств коммуникации породили организованные формы онлайн-мошенничества. Примитивные формы мошенничества сменяются все более изощренными, новые технологии проникают в нашу жизнь, так появились формы мошенничества с использованием chat gpt, то есть нейросетей. Вышеназванные обстоятельства обосновывают актуальность темы исследования. Предметом исследования являются различные виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения. Новизна темы публикации обусловлена необходимостью тщательного исследования новых организованных форм онлайн-мошенничества для предупреждения совершения таких преступлений. Впервые исследована «модификация» как способ компьютерного мошенничества, нейросеть, как способ совершения мошенничества. Предпринята попытка охарактеризовать организованную преступную группу, совершающую онлайн-мошенничество. Исследованы цифровые следы организованных форм онлайн-мошенничества. Целью настоящей публикации является выделение особенностей совершения организованных форм онлайн-мошенничества. Их выделение поможет эффективному раскрытию таких преступлений. В статье используются различные методы: всеобщий диалектический, логический, анализа нормативно-правового регулирования, формально-юридический , сравнительно-правовой. Выводы: на основе теории и правоприменительной практики определены ключевые элементы организованных форм онлайн-мошенничества, охарактеризованы ключевые особенности организованных преступных групп, их совершающих, установлена роль нейросетей в совершении рассматриваемых преступлений.

**Ключевые слова:**

онлайн-мошенничество, компьютерное мошенничество, нейросеть, модификация, организованная группа, цифровые следы, правоприменительная практика, цифровизация, компьютеризация, новелла

**Введение.** Мошенничество в сфере компьютерной информации согласно букве закона является хищением чужого имущества или приобретением права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ч. 1 ст. 159.6 УК РФ). Иными словами, под чистого рода хищение оно подпадает только в первой части формулировки, поскольку предполагается вариант «или приобретение права на чужое имущество». При этом способы совершения преступления уже названы в законе и охарактеризованы в научной литературе [1, с. 43]. Изучением проблем онлайн-мошенничества: мошенничества в сфере компьютерной информации и использования высоких технологий занимались следующие ученые: Русскевич Е.А., Фролов М.Д., Шевченко Е.С., Тропина Т.Л. и другие.

**Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения.** Мошенничество в сфере компьютерной информации и использования высоких технологий в последнее время набирает все большие обороты [3, с. 22] и

достаточно примитивные формы обмана сменяются наиболее изощренными сценариями введения в заблуждение потерпевших. Если прежде телефонные обзвоны на предмет того, что якобы близкий родственник абонента попал в беду (стал жертвой дорожно-транспортного происшествия или угадил в полицию) были ориентированы на доверчивого потерпевшего и нередко срабатывали с людьми старшего и преклонного возраста, то в настоящее время использование возможностей нейросети открывает поистине безграничные возможности. От фейковых новостей, мошенничества и вымогательства под «продажу компрометирующих» видеоматериалов, до видеозвонков с моделированием точного изображения внешнего облика якобы звонящего близкого родственника – вот только не полный перечень тех направлений, где преступники могут приложить в полной мере свой криминальный талант. Нейросеть как инструмент искусственного интеллекта, которому под силу решение сложнейших задач, уже используется для розыгрышей, создания фейковых новостей и распространения порочащих честь и достоинство знаменитостей видеоматериалов. Поэтому высокоорганизованное мошенничество не останется в стороне от этих дополнительных ресурсов приложения преступных усилий. Важно понимать, что здесь нет традиционного для мошенничества обмана и введения в заблуждение, но злоумышленники все-таки используют недостаточную компьютерную грамотность пользователей и излишнюю их уверенность в собственной информационной безопасности. И так, злоумышленники прибегают к удалению (в ст. 272 УК РФ используется синонимичный термин «уничтожение») компьютерной информации с тем, чтобы добиться ее потери законным пользователем. Однако потеря далеко не всегда означает невозможность восстановления утраченных данных. Напротив, блокирование компьютерной информации осуществляется не с целью повлиять на качественные и количественные характеристики самой компьютерной информации, а для того, чтобы ограничить доступ или вовсе не допустить к этим ресурсам законного пользователя. Следствием блокировки компьютерной информации становится невозможность временного или постоянного получения доступа к этим данным, т.е. не происходит изменение содержания информации, которая остается нетронутой, но становится недоступной [2, с. 66]. Модификация как способ совершения компьютерного мошенничества является средством полного или частичного видоизменения информации. Под иным вмешательством с точки зрения реализации намерений по осуществлению компьютерного мошенничества в практике зачастую понимают неправомерный доступ к компьютерной информации, ее копирование, если таковые приводят к хищению чужого имущества или приобретения прав на него.

Тем не менее, традиционные компьютерные и в целом высокотехнологичные виды мошенничества остаются в своем сегменте наиболее востребованными среди нечистых на руку дельцов [4, с. 32]. Взлом аккаунтов позволяет мошенникам получить базу данных о знакомых его владельца, которым, как правило, рассылаются письма с просьбой оказать помощь в сложной жизненной ситуации. При этом, мошенники не гнушаются ничем: тяжелое состояние ребенка после дорожно-транспортного происшествия, пожар, где сгорели все близкие и имущество и пр. И чем чудовищнее объяснения под необходимость пожертвования, тем легче откликаются особенно неблизкие знакомые и перечисляют средства на счет мошенников. Близкие, как правило, пытаются созвониться с жертвой взлома акаунта в соцсетях и тогда обман вскрывается.

Нередко в поле зрения правоохранительных органов попадают только рядовые исполнители из организованной преступной группы, тогда как «интеллектуальный центр» в лице ее руководства зачастую выявить не удается. Максимальная анонимность,

использование псевдонимов и прозвищ, «цифровизация» своего участия [5, с. 65] в реализации общей схемы компьютерного мошенничества создают эффективную защиту от уголовного преследования. В частности, по деятельности одной из таких преступных группировок сложилась вполне стандартная для дел подобного рода ситуация. Неустановленные члены организованной группы под руководством участника, действующего под псевдонимом «Директор», обладающие специальными знаниями и навыками в сфере компьютерной информации, с преступными намерениями прибегли к распределению и использованию компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования и нейтрализации средств защиты компьютерной информации. С помощью этих программ был обеспечен неправомерный доступ к локальной сети определенного «Директором» в качестве объекта преступного посягательства коммерческого банка, и соответственно – к командному серверу банковской локальной сети с персональными компьютерами сотрудников банка и внешних (периферийных) устройств – банкоматов. С помощью тех же деструктивных программ преступники получили доступ к управлению банкоматами, в том числе, путем направления им неправомерных команд на выдачу наличных денег без использования платежных банковских карт. Высокая организация преступной группы не предусматривала обязательное личное знакомство ряда ее участников друг с другом и руководителем, что обеспечивало конспирацию и никаким образом не мешало эффективности преступной деятельности. При этом взаимоотношения участников группы отличались высоким уровнем взаимного доверия и сплоченности. Высокая степень координации совместных усилий, точность исполнения криминальных ролей обеспечивали успешное совершение планируемых преступлений и распределение похищаемых денежных средств от непосредственных их получателей в банкоматах до руководителя. Организованная преступная группа отличалась устойчивостью, выразившейся в стабильности ее состава на протяжении длительного времени[1].

Характерным для компьютерного мошенничества по мнению некоторых ученых является то, что в ходе его осуществления и по результатам приложения преступных усилий не возникает особо острой необходимости скрывать следы преступления, поскольку рано или поздно выявление ущерба становится очевидным. Такого мнения придерживаются, например, Русскевич Е.А. и Фролов М.Д. Мы не можем согласиться с данными учеными, так как именно в организованных формах онлайн-мошенничества сокрытие следов может осуществляться через зарубежные серверы информации или сервисов GPT. А согласно собственной правоприменительной практике автора иногда следы скрываются в сговоре с самими сотрудниками онлайн-субъекта. Добросовестный и профессиональный сотрудник службы безопасности немедленно отреагирует и поведет себя в соответствии с должностной инструкцией, тогда как тот работник, который участвует в реализации преступной схемы даже при очевидности причиненного ущерба будет скрывать произошедшее. При этом, само сокрытие следов изначально заложено в способах реализации преступных намерений, поскольку максимальная законспирированность главных действующих лиц преступной группы, ее организаторов, дистанцирование их от рядовых исполнителей и отсутствие личных и уж тем более близких контактов создают необходимые условия для их защиты от уголовного преследования.

Нередко сложность в доказывании причастности к преступлению конкретных организаторов возникает в связи с существующей негласной, но от этого не менее императивной, «корпоративной солидарностью», которая выстраивается на том, что находящийся под следствием исполнитель, пособник, и намного реже – подстрекатель, не без оснований рассчитывает на юридическую помощь и коррупционные связи своего покровителя, организатора преступной группы. Такая корпоративная солидарность

присуща большинству преступных групп мошенников, поскольку нередко эта надежда на поддержку «с воли» оказывается более сильным мотивом, нежели предусмотренные законом преференции, когда, к примеру, досудебное соглашение о сотрудничестве выглядит куда как менее убедительным стимулом в содействии органам расследования и дознания в решении задач изобличения всех виновных в содеянном. Кроме того, преданность корпоративным интересам преступной группы нередко стимулируется возможностью поучаствовать в распределении криминальной прибыли уже после освобождения из заключения. Нередко попавшие в сферу уголовного преследования рядовые члены мошеннической преступной группы просто не могут покинуть порочный круг, поскольку по выходу на свободу им просто некуда будет вернуться. Это характерно в особенности для национально-этнических преступных групп мошенников.

**Заключение.** И так, в сфере реализации высокоорганизованных преступных технологий компьютерного мошенничества выделяются следующие особенности: 1) тщательная подготовка в виде анализа системы защиты банка, иного хозяйствующего субъекта, разработки плана реализации преступных намерений и сокрытия факта участия в нем конкретных лиц, приискания и отладки соответствующего оборудования и программного обеспечения, вовлечения соучастников и распределение между ними ролей, степени и форм участия каждого, четкой алгоритмизации совместных действий к достижению преступного результата, проработки дележа полученной преступной прибыли и разного уровня отмывание преступного дохода; 2) применение высокого уровня специальных знаний при использовании компьютерного оборудования и программного обеспечения в преступных целях; 3) максимальная дистанцированность от личных контактов участников преступной группы; 4) легендирование законности полученного преступного дохода и отмывание денежных средств, полученных такого рода криминальным путем; 5) быстрота и высокая эффективность предпринимаемых мошенниками действий, направленных на достижение преступного результата.

[1] Приговор Якутского городского суда Республики Саха (Якутии) от 26 августа 2019 г. по уголовному делу № 1-1462/2018 по обвинению Булахова Д.Д. и Булахова И.Д. в совершении преступлений, предусмотренных ч.3 ст. 272, ч.2 ст. 273 и ч.4 ст. 159.6 УК РФ.

## Библиография

1. Драпкин Л.Я. Криминалистика / под ред. Л.Я. Драпкина. М: Юрайт, 2012.
2. Русскевич Е.А., Фролов М.Д. Мошенничество в сфере компьютерной информации: монография. М.: НИЦ ИНФРА-М, 2020.
3. Шевченко Е.С. Тактика отдельных следственных действий при расследовании киберпреступлении // Закон и право. 2015. № 8. С. 128-138.
4. Тропина Т. Л. Компьютерное мошенничество: вопросы квалификации и законодательной техники. М., 2006.
5. Цифровизация экономических систем: теория и практика: монография / под ред. д-ра экон. наук, проф. А. В. Бабкина. – СПб.: ПОЛИТЕХ-ПРЕСС, 2020.

## Результаты процедуры рецензирования статьи

*В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.*
*Со списком рецензентов издательства можно ознакомиться здесь.*

Предметом исследования в представленной на рецензирование статье, как это следует из ее наименования, должны были являться организованные формы (т.е. внешние проявления, виды) онлайн-мошенничества. Перечислению этих форм посвящена вводная часть работы. В основной части статьи автор фактически выявил особенности данного вида преступлений, которые в итоге перечисляются в заключительной части статьи. Таким образом, наименование работы не соответствует ее фактическому содержанию и должно быть уточнено.

Методология исследования в тексте статьи не раскрывается, но очевидно, что ученым использовались всеобщий диалектический, логический, формально-юридический, герменевтический методы исследования.

Актуальность избранной автором темы исследования во вводной части работы не обоснована, хотя в начале основной части статьи содержится следующее положение: "Мошенничество в сфере компьютерной информации и использования высоких технологий в последнее время набирает все большие обороты [3, с. 22] и достаточно примитивные формы обмана сменяются наиболее изощренными сценариями введения в заблуждение потерпевших". Также ученому необходимо перечислить фамилии ведущих специалистов, занимавшихся исследованием поднимаемых в статье проблем, и раскрыть степень их изученности.

В чем проявляется научная новизна работы, прямо не говорится. Фактически она отражается в некоторых заключениях автора: "... в сфере реализации высокоорганизованных преступных технологий компьютерного мошенничества выделяются следующие особенности: 1) тщательная подготовка в виде анализа системы защиты банка, иного хозяйствующего субъекта, разработки плана реализации преступных намерений и сокрытия факта участия в нем конкретных лиц, приискания и отладки соответствующего оборудования и программного обеспечения, вовлечения соучастников и распределение между ними ролей, степени и форм участия каждого, четкой алгоритмизации совместных действий к достижению преступного результата, проработки дележа полученной преступной прибыли и разного уровня отмывание преступного дохода; 2) применение высокого уровня специальных знаний при использовании компьютерного оборудования и программного обеспечения в преступных целях; 3) максимальная дистанцированность от личных контактов участников преступной группы; 4) легендирование законности полученного преступного дохода и отмывание денежных средств, полученных такого рода криминальным путем; 5) быстрота и высокая эффективность предпринимаемых мошенниками действий, направленных на достижение преступного результата". Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и заслуживает внимания читательской аудитории.

Научный стиль исследования выдержан автором в полной мере.

Структура работы не вполне логична. Вводная часть исследования практически отсутствует. В основной части статьи автор на основании анализа некоторых теоретических источников и материалов судебной практики выявляет ряд особенностей мошенничеств в сфере компьютерной информации и использования высоких технологий. В заключительной части статьи содержатся выводы по результатам проведенного исследования.

Содержание статьи, как уже было отмечено, не соответствует ее наименованию.

Библиография исследования представлена 5 источниками (монографиями, научной статьей и учебником). С формальной точки зрения этого достаточно. Фактически автору необходимо привести в соответствие наименование работы и ее содержание.

Апелляция к оппонентам отсутствует, что недопустимо для научной статьи. Автор ссылается на ряд источников исключительно в подтверждение своих суждений либо для иллюстрирования отдельных положений работы. В научную дискуссию он не вступает.

Выводы по результатам проведенного исследования имеются ("И так, в сфере реализации высокоорганизованных преступных технологий компьютерного мошенничества выделяются следующие особенности: 1) тщательная подготовка в виде анализа системы защиты банка, иного хозяйствующего субъекта, разработки плана реализации преступных намерений и сокрытия факта участия в нем конкретных лиц, приискания и отладки соответствующего оборудования и программного обеспечения, вовлечения соучастников и распределение между ними ролей, степени и форм участия каждого, четкой алгоритмизации совместных действий к достижению преступного результата, проработки дележа полученной преступной прибыли и разного уровня отмывание преступного дохода; 2) применение высокого уровня специальных знаний при использовании компьютерного оборудования и программного обеспечения в преступных целях; 3) максимальная дистанцированность от личных контактов участников преступной группы; 4) легендирование законности полученного преступного дохода и отмывание денежных средств, полученных такого рода криминальным путем; 5) быстрота и высокая эффективность предпринимаемых мошенниками действий, направленных на достижение преступного результата"), являются достоверными и обоснованными, и, безусловно, заслуживают внимания потенциальных читателей.
Статья нуждается в дополнительном вычитывании. В ней встречаются опечатки.
Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере уголовного права и криминологии при условии ее доработки: уточнении наименования работы и ее структуры, раскрытии методологии исследования, обосновании актуальности его темы, введении элементов дискуссионности, устранении нарушений в оформлении статьи.

## Результаты процедуры повторного рецензирования статьи

*В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.*
*Со списком рецензентов издательства можно ознакомиться здесь.*

На рецензирование представлена научная статья с наименованием «Организованные формы онлайн-мошенничества: виды мошенничества в сфере компьютерной информации и использования высоких технологий и особенности их совершения» для опубликования в журнале «Юридические исследования». Текст статьи, тематика, структура документа соответствуют шифру научной специальности 5.1.4 «Уголовно-правовые науки» в части научного исследования по паспорту п. 3: Теория уголовного права: уголовно-правовое регулирование; преступление, уголовная ответственность; применение уголовного права; социальная обусловленность и эффективность уголовного права, закономерности и тенденции его развития и совершенствования», а также требованиям научного журнала в части актуальности, новизны, способности вызвать интерес у читательской аудитории.
Так, в качестве предмета исследования автор в своей статье предлагает к изучению высокотехнологичные способы совершения онлайн–мошенничеств, что относится к закономерностям совершения преступлений в онлайн-пространстве. Также автор подкрепляет свои выводы по предмету исследования теоретическими изысканиями ученых–исследователей по заданной теме и практическими аргументами, что укладывается в классическую «схему» изучения указанного предмета. Методология исследования основана на системе общенаучных и частных научных методов. В статье использовались при изложении материала и формулировании выводов метод логического осмысления; при анализе следственно-судебной практики использован статистический метод.

Актуальность рецензируемого исследования не вызывает сомнений, поскольку развитие высоких технологий, изворотливость преступников в пространстве сети Интернет, доверчивость граждан и техническое, кадровое отставание правоохранительных органов уже много лет являются «благодатной почвой» для кибер-преступников. Автор правильно отмечает наличие правовых и теоретических пробелов, которые усугубляют ситуацию и повышают уровень необходимости их нивелирования.

Научная новизна статьи заключается в проведенном комплексном исследовании организованных форм онлайн-мошенничеств, их видов, способов и особенностей совершения и формулирования авторской системы особенностей предмета исследования, а также обстоятельств, подлежащих обязательному установлению по указанному виду преступного посягательства. Все это в целом имеет важное теоретическое и практическое значение.

Стиль написания текста носит научный характер. Структура представлена введением, основным содержанием и заключением, что соответствует требованию, предъявляемому к научным статьям. Содержание статьи соответствует заявленной тематике и характеру подлежащих исследованию вопросов.

В работе использованы труды ученых-специалистов в изучаемой сфере. Использованные монографические исследования относятся к современному периоду развития научной мысли. Всего использовано пять источников из теоретических исследований, а также нормативно-правовые акты и судебная практика. Поэтому библиографический перечень соответствует предъявляемым требованиям.

Выводы, сделанные автором статьи, заслуживают внимания и одобрения у читательской аудитории из числа обучающихся вузов, ученых и практических работников органов правопорядка.

Научная статья может быть рекомендована к опубликованию.