Светлана Михайловна ГОЛЯТИНА,
кандидат юридических наук, ORCID 0000-0001-6077-9827
Волгоградская академия МВД России (г. Волгоград)
доцент кафедры криминалистики учебно-научного комплекса
по предварительному следствию в органах внутренних дел
sgoliatina@mvd.ru

Научная статья
УДК 343.9:345.85[343.72:004]

КРИМИНАЛИСТИЧЕСКОЕ ПРОГНОЗИРОВАНИЕ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

КЛЮЧЕВЫЕ СЛОВА. Киберпреступность, дистанционное мошенничество, кибермошенничество, дипфейк, прогноз, криминалистическое прогнозирование, прогнозный фон, способ совершения преступления.

АННОТАЦИЯ. ***Введение.*** *В настоящее время киберпреступность в целом и кибермошенничество в частности признаны национальной проблемой. Число преступлений этого вида растет из года в год, ущерб от них исчисляется миллиардами рублей, их жертвами становится всё больше людей – от несовершеннолетних до пенсионеров. Совершенствование технологий искусственного интеллекта открыло перед злоумышленниками новые возможности для совершения преступлений. Понимание тенденций развития киберпреступности позволяет выработать стратегии борьбы с ней и оценить эффективность мер по ее предупреждению и профилактике, по противодействию ей.* ***Методы.*** *В ходе исследования применялись: диалектический метод, необходимый для полного и всестороннего изучения явлений, связей и противоречий между ними, а также описание, логические методы (анализ и синтез, индукция и дедукция), статистический метод, методы криминалистического прогнозирования.* ***Результаты.*** *На основании выводов, сделанных по итогам изучения научной литературы по теме исследования, автором сформулировано понятие криминалистического прогнозирования. Таковым представляется научно обоснованное предвидение изменений в характере преступлений, способах их совершения, а также возможных направлений дальнейшего развития методов и приемов борьбы с преступностью, технико-криминалистических средств, используемых при расследовании преступлений, и криминалистической науки в целом. Руководствуясь этим определением, автор исследовала историю развития киберпреступности в России. Отмечены причины и условия, способствующие росту показателей, характеризующих данный вид преступности, составлен криминалистический прогноз развития ситуации на ближайшее будущее. Выявлены тенденции, связанные с практикой осуществления дистанционного мошенничества, намечены вероятные пути дальнейшего изменения мошеннических схем. Всё это необходимо для разработки эффективной системы упреждающих мер, что должно способствовать повышению действенности профилактики преступлений рассматриваемого вида.*

ВВЕДЕНИЕ

Дистанционные мошенничества в последние годы стали серьезной проблемой для граждан и правоохранительных органов России. В 2023 году на территории нашей страны было зарегистрировано 677 тысяч киберпреступлений, что на 29,7% больше, чем в 2022 году; ущерб от действий злоумышленников составил 156 млрд рублей[1]. Большая часть таких преступлений (53%) пришлась на мошенничества[2]. С ними в 2023 году столкнулся 91% россиян. С платежных карт преступникам удалось похитить 7,1 млрд рублей, с банковских счетов – 4,6 млрд рублей, через систему быстрых платежей – 3,3 млрд рублей, с электронных кошельков – 105,2 млн рублей[3]. В число используемых чаще всего технологий обмана граждан входили: схема с «безопасным» счетом [1], обещания сверхприбыли на бирже [2], финансовые пирамиды [3], фишинг [4] и др.

Заместитель председателя правления «Сбербанка» С. Кузнецов по этому поводу сказал: «По-прежнему наиболее актуальными и опасными

[1] За пять лет число киберпреступлений увеличилось более чем вдвое // Российская газета: сайт. 25.09.2024 // URL: https://rg.ru/2024/09/25/policiia-v-seti.html (дата обращения: 01.11.2024).
[2] Катаева В., Поляков Д. Россия – одна из стран с очень высоким уровнем киберугроз. Но до полиции доходит меньше половины преступлений, и только четверть из них раскрывают // Если быть точным: сайт // URL: https://tochno.st/materials/rossiia-odna-iz-stran-s-ocen-vysokim-urovnem-kiberugroz-no-do-policii-doxodit-mense-poloviny-prestuplenii-i-tolko-cetvert-iz-nix-raskryvaiut (дата обращения: 01.11.2024).
[3] Павлова М. 8 фактов о мошенничестве в России: от финансовых пирамид до кибератак // Т–Ж: сайт. 30.05.2024 // URL: https://journal.tinkoff.ru/short/ne-obmanuly/ (дата обращения: 01.11.2024).

Svetlana M. GOLYATINA,
Cand. Sci. (Jurisprudence), ORCHID 0000-0001-6077-9827
Volgograd Academy of the Ministry of the Interior of Russia (Volgograd, Russia)
Associate Professor of the Department of Criminalistics of the Educational
and Scientific Complex for Preliminary Investigation in the Internal Affairs Bodies
sgoliatina@mvd.ru

CRIMINALISTIC FORECASTING REMOTE FRAUD

KEYWORDS. Cybercrime, remote fraud, cyber fraud, deepfake, forecast, forensic forecasting, forecast background, crime method.

ANNOTATION. ***Introduction.*** *Currently, cybercrime in general and cyberfraud in particular are recognized as a national problem. The number of crimes of this type is growing from year to year, the damage from them is estimated at billions of rubles, more and more people are becoming their victims – from minors to pensioners. Improvement of artificial intelligence technologies has opened up new opportunities for criminals to commit crimes. Understanding the trends in the development of cybercrime allows us to develop strategies to combat it and assess the effectiveness of measures to prevent and combat it.* ***Methods.*** *The study used: the dialectical method, necessary for a complete and comprehensive study of phenomena, relationships and contradictions between them, as well as description, logical methods (analysis and synthesis, induction and deduction), statistical method, forensic forecasting methods.* ***Results.*** *Based on the conclusions made from the study of scientific literature on the topic of the study, the author formulated the concept of forensic forecasting. This is a scientifically based prediction of changes in the nature of crimes, methods of their commission, as well as possible directions for further development of methods and techniques for combating crime, technical and forensic tools used in investigating crimes, and forensic science in general. Guided by this definition, the author studied the history of cybercrime development in Russia. The reasons and conditions contributing to the growth of indicators characterizing this type of crime are noted, a forensic forecast for the development of the situation in the near future is compiled. Trends associated with the practice of remote fraud are identified, probable ways of further changing fraudulent schemes are outlined. All this is necessary for the development of an effective system of preventive measures, which should contribute to increasing the effectiveness of preventing crimes of this type.*

мошенническими схемами являются звонки по телефону и через мессенджеры от имени сотрудников правоохранительных органов и Центрального банка России с требованием перевода денег на безопасный счет. Тут есть два пути возможного развития событий: мошенники либо запрашивают данные карты, пароли из СМС и другую информацию, чтобы самим похитить деньги, либо убеждают людей самостоятельно совершать операции: переводы, снятие и зачисление денег в банкоматах, оформление кредитов»[1].

В 2023 году злоумышленники провели 1,17 млн успешных операций. По данным Центрального банка России, причина сложившейся ситуации состоит в том, что киберпреступники осуществляют хорошо подготовленные адресные атаки[2]. Вместе с тем на положение дел негативное влияние оказывает то, что наряду с уже привычными и, к сожалению, в большинстве случаев безотказно работающими методами мошенничества начинают использоваться новые, изощренные, технологичные и многоходовые, например хищения денежных средств путем обмана или злоупотребления доверием, совершаемые с использованием генеративно-состязательных сетей – нейронных сетей, которые умеют генерировать музыку, изображения, речь и тексты, и технологии «дипфейк» [5]. Н.И. Старостенко пишет: «Анализ судебно-следственной практики в России не выявил фактов многократного использования технологий «deepfake» при совершении хищений, но их существование, активная разработка и внедрение позволяют сделать вывод об их соответствии потребностям злоумышленников, совершающих мошеннические действия, а также прогнозировать их широкое применение в корыстных целях на ближайшую перспективу» [6, с. 189].

Какие еще способы совершения дистанционного мошенничества могут появиться в ближайшее время? Какие трансформации ждут киберпреступность? Каковы тенденции ее развития? Ответы на эти вопросы помогает найти криминалистическое прогнозирование – научно обоснованное предвидение изменений в характере преступлений, способах их совершения, а также возможных направлений дальнейшего развития методов и приемов борьбы с преступностью, технико-криминалистических средств, используемых при расследовании преступлений, и криминалистической науки в целом.

МЕТОДЫ

Методологическую основу исследования, результаты которого представлены в настоящей статье, составил диалектический метод. Он был необходим для полного и всестороннего изучения явлений, связей и противоречий между ними. Кроме того, оказалась востребована совокупность обще- и частнонаучных методов: описание – для

[1] Шаповалова А. Зампред Сбера рассказал о воздействии мошенников на эмоции людей // Лента.ру: сайт. 04.09.2024 // URL: https://lenta.ru/news/2024/09/04/rasskazal/ (дата обращения: 01.11.2024).
[2] Корочкина А. Кибермошенники украли почти 16 млрд руб. у россиян в 2023 году // Forbes: сайт. 13.02.2024 // URL: https://www.forbes.ru/finansy/506131-kibermosenniki-ukrali-pocti-16-mlrd-rublej-u-rossian-v-2023-godu (дата обращения: 01.11.2024).

характеристики материала, логические методы (анализ и синтез, индукция и дедукция) – для последовательного и понятного изложения фактов, статистический метод – для анализа количественных показателей, методы криминалистического прогнозирования (аналогия, экстраполяция, моделирование) и др.

РЕЗУЛЬТАТЫ

Впервые о криминалистическом прогнозировании как о самостоятельном направлении криминалистической науки начали говорить еще в 1939 году, когда С.А. Голунский и Б.М. Шавер выдвинули гипотезу о возможности определения новых способов совершения преступлений на основе изучения данных о расследовании их отдельных видов[1]. Позднее это предположение получило развитие в трудах Р.С. Белкина, который определил объекты прогнозирования. К их числу он отнес способы совершения преступлений, следы, обстановку совершения преступлений, особенности поведения фигурантов уголовного дела, технико-криминалистические средства и тактические приемы, следственные ситуации, методики расследования преступлений и т.д.[2]

Центральное место способу совершения преступлений в структуре криминалистического прогнозирования отводил Г.Г. Зуйков. На его взгляд, способом надлежит именовать «систему действий по подготовке, совершению и сокрытию преступлений, детерминированных условиями внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий или средств и условий места и времени»[3]. Схожего мнения придерживается А.А. Бессонов. По его мнению, в структуру способа преступления входят «действия преступника (его соучастников) по подготовке, совершению и сокрытию преступления, объединенные единым преступным замыслом или отношением к последствиям; взаимосвязь этих действий с объектом (предметом) посягательства, условиями окружающей преступление обстановки и свойствами личности преступника; приемы, орудия и средства совершения преступных действий; отражение этих действий в объективной реальности в виде следов» [7, с. 173].

Основываясь на приведенных точках зрения, используя сведения о существующих в настоящее время способах (схемах) совершения дистанционных мошенничеств, рассмотрим данный вид преступных посягательств с позиции криминалистического прогноза.

Обычно подготовка такого прогноза включает в себя несколько этапов.

Первый – прогнозная ретроспекция. Здесь происходит анализ истории развития прогнозного объекта и внешних факторов, влияющих на него, – прогнозного фона. Киберпреступность – явление не новое, она возникла еще в 1960-е годы, когда представляла собой попытки взлома операционных систем и получения доступа к конфиденциальной информации [8]. Позднее злоумышленники стали использовать в криминальных целях вредоносное программное обеспечение, фишинг, DDoS-атаки, социальную инженерию и т.д. Сегодня данный перечень пополнился технологиями искусственного интеллекта. В России впервые о киберпреступности заговорили в 90-е годы XX века, когда был зарегистрирован домен «.ru» и началось активное внедрение Интернета во многие сферы общественной жизни. Всеобщие цифровизация и компьютеризация, переход бизнеса в интернет-среду, развитие интернет-торговли, информационные поводы, дающие мошенникам возможность обогатиться, недостатки в работе правоохранительных органов вместе с низким уровнем финансовой грамотности населения, отсутствием у большинства граждан навыков цифровой гигиены и несерьезным отношением к интернет-преступности обусловили ее стремительный рост (см. схему 1). При этом важно отметить, что на протяжении многих лет большую часть киберпреступлений составляют именно кибермошенничества.

Второй этап криминалистического прогнозирования называется прогнозным диагнозом. На нем выявляются тенденции развития объекта прогнозирования и прогнозного фона. В 2023-2024 годах Россия заняла первое место в мире по числу телефонных мошенничеств. Это подтверждают и представители «Сбербанка»: «Мы имеем мировое лидерство с точки зрения потерь, с точки зрения масштабов бедствия от телефонного мошенничества»[4]. По словам заместителя председателя правления «Сбербанка» С. Кузнецова, ежедневно злоумышленники совершают до 20 млн звонков: «Такого масштаба атак на наших граждан не было никогда. Примерно в одном случае из ста люди верят телефонным мошенникам. То есть порядка 200 тысяч граждан в сутки могут попадаться на их обман»[5].

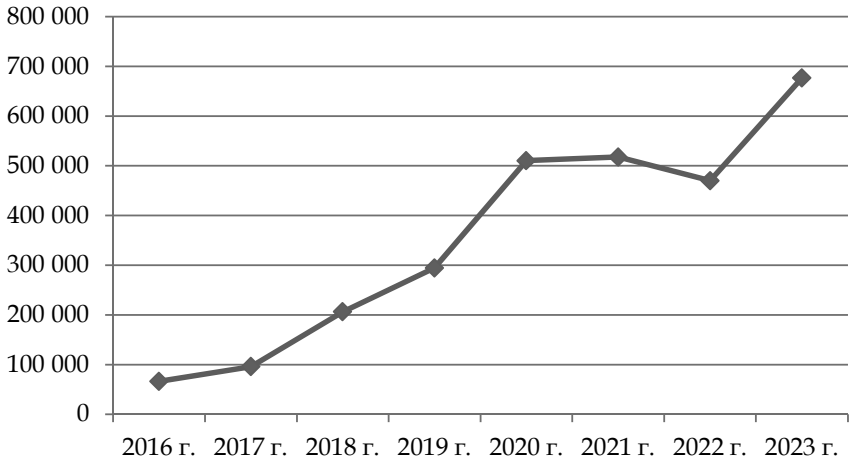
Наиболее часто используются следующие схемы дистанционного мошенничества:

- «FakeBoss»: человек получает сообщение якобы от руководителя организации, где он работает, который предупреждает его о предстоящем звонке из правоохранительных органов. Далее гражданину звонит мнимый правоохранитель, информирует потенциальную жертву о ее уча-

[1] Голунский С.А., Шавер Б.М. Криминалистика. Методика расследования отдельных вдов преступлений: Учебник. М.: Юрид. изд-во НКЮ СССР, 1939. 372 с.
[2] Белкин Р.С. Ленинская теория отражения и методологические проблемы советской криминалистики: Учебное пособие по курсу советской криминалистики. М.: ВШ МВД СССР, 1970. 130 с.
[3] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: Автореф. дис. ... докт. юрид. наук. М., 1970. С. 10.
[4] Костерева М. Сбербанк заявил о лидерстве России по масштабам ущерба от телефонных мошенников // Коммерсантъ: сайт. 06.06.2024 // URL: https://www.kommersant.ru/doc/6747796 (дата обращения: 01.11.2024).
[5] Романова Т. В Сбере назвали критической ситуацию с телефонным мошенничеством // Лента.ру: сайт. 04.07.2024 // URL: https://lenta.ru/news/2024/06/04/kriticheskoy/ (дата обращения: 25.11.2024).

Схема 1. Количество киберпреступлений, зарегистрированных в России в 2016-2023 гг. (по данным МВД России*)

* Состояние преступности: статистика и аналитика // МВД России: сайт // URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 25.11.2024).



стии в мошеннической схеме и предлагает перевести деньги на «безопасный» счет. Затем следует звонок от «сотрудника банка», который советует продать имущество или оформить кредит. В результате человек переводит некую сумму на указанный мошенниками счет и лишь после этого осознает, что стал жертвой обмана [9];

- имитация голоса родных и близких в аудиосообщениях (голоса генерируются с помощью технологии «дипфейк») [9];

- звонки по видеосвязи для идентификации клиентов банка по биометрии [10];

- звонки по видеосвязи якобы из правоохранительных органов и специальных служб [11].

Приведем несколько примеров. 75-летней жительнице г. Чебоксары позвонил по видеосвязи ее бывший коллега (как выяснилось позже, изображение было сгенерировано нейросетью) и сообщил, что в образовательной организации, где она раньше работала, проводится служебное расследование. После этого ей поступил видеозвонок от сотрудника правоохранительных органов (его изображение также было сгенерировано). Он предъявил служебное удостоверение и убедил женщину перевести 500 тысяч рублей на «безопасный» счет, чтобы не допустить их отправки на Украину. Чтобы найти недостающие средства, ей посоветовали обратиться к знакомым. В результате на счет мошенников пенсионерка перевела почти миллион рублей[1]. От жительницы г. Барнаула М. ее родственникам, друзьям и знакомым стали приходить голосовые и видеосообщения с просьбой одолжить ей денег. Как оказалось позже, когда на счет злоумышленников уже были отправлены совокупно 100 тысяч рублей, аккаунт М. был взломан, а ее голос и внешность – результат работы нейросети[2]. Жительница г. Зуевки Кировской области перевела на счет злоумышленников 300 тысяч рублей. По ее словам, по видеосвязи ей позвонил сотрудник спецслужб, за его спиной висел портрет Президента Российской Федерации В.В. Путина, данный факт натолкнул женщину на мысль о том, что она разговаривает с настоящим силовиком. Позже этот же преступник, который выглядел как актер Р. Дауни-младший и представился полицейским, попытался выманить деньги у мужчины, но потерпел неудачу[3].

Отметим, что с начала 2024 года число преступных схем с использованием дипфейков выросло в 30 раз[4].

Обеспокоенность вызывают не только дипфейки, но и появляющиеся схемы мошенничества с цифровым рублем (хотя в настоящее время он существует только в тестовом режиме). Член комитета Государственной Думы Федерального Собрания Российской Федерации по информационной политике А. Немкин отметил, что «в различных целях злоумышленники могут создавать поддельные приложения или веб-сайты, которые выглядят как официальные платформы для работы с цифровым рублем. Пользователи, вводя свои данные, могут неосознанно передать их мошенникам. Также гражданам могут поступать предложения «инвестиционных возможностей» с использованием цифрового рубля с обещаниями высокой прибыли. Пользователи могут вложить свои деньги, но в итоге потерять их»[5]. Иными словами, схемы мошенничества здесь в целом такие же, как в случае с безналичными денежными средствами.

После внесения изменений в Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (внедрение «периода охлаждения», отключение каналов дистанционного банковского обслуживания «дропам»[6]) мошенни-

[1] Зейналов А. Жительница Чебоксар перевела мошенникам почти миллион рублей, поверив в дипфейк // Коммерсантъ: сайт. 14.11.2024 // URL: https://www.kommersant.ru/doc/7299409 (дата обращения: 14.11.2024).
[2] Усик А. «Взломать могут любого». От имени жительницы Барнаула разослали дипфейки с просьбой занять денег // Комсомольская правда: сайт. 30.09.2024 // URL: https://www.alt.kp.ru/daily/27640.5/4990570/ (дата обращения: 02.11.2024).
[3] Джабборов Д. Мошенник с лицом Роберта Дауни-младшего попытался украсть деньги кировчанина // Газета.ru: сайт. 22.03.2024 // URL: https://www.gazeta.ru/tech/news/2024/03/22/22608199.shtml (дата обращения: 02.11.2024).
[4] Состояние преступности: статистика и аналитика // МВД России: сайт // URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 25.11.2024).
[5] Денисенко А. В России выстроены первые схемы мошенничества с цифровым рублем // CNews: сайт. 04.07.2024 // URL: https://www.cnews.ru/news/top/2024-07-04_v_rossii_poyavilis_pervye (дата обращения: 25.11.2024).
[6] Дроп – от англ. to drop «сбрасывать»; «дропами» злоумышленники называют людей, с помощью которых они прячут украденное.

ки стали использовать новую схему: они убеждают россиян снимать деньги со счетов и передавать их «инкассаторам», которые якобы перевезут наличные в другой банк на хранение (вместо перевода на «безопасный» счет). Такая схема позволяет злоумышленникам обойти антифрод-проверки и потому набирает популярность [12]. По информации сервиса «DLBI», на нее уже приходится около 80% всех случаев хищений[1]. Из сказанного можно сделать вывод о том, что киберпреступность продолжает развиваться и адаптируется к новым вызовам и технологиям.

Третий этап криминалистического прогнозирования – проспекция. Здесь происходит разработка прогнозов на основе диагноза. С учетом статистических данных о состоянии киберпреступности в стране, схем мошенничества, которые приспосабливаются к условиям окружающей социальной среды, по-прежнему недостаточно высокого уровня цифровой и финансовой культуры населения (особенно социально незащищенных категорий граждан) полагаем, что число дистанционных мошенничеств в ближайшее время будет расти. По нашему мнению, сценарии со звонками от «сотрудников правоохранительных органов» и «представителей Центробанка России» с рекомендациями перевести денежные средства на «безопасный» счет или отдать их «инкассаторам» будут активно использоваться злоумышленниками, так как эти схемы просты в исполнении и, несмотря на профилактическую работу со стороны государства, вот уже на протяжении нескольких лет приносят преступникам самую большую прибыль. Стремительное развитие технологии искусственного интеллекта и других инноваций, которые киберпреступники могут использовать в своих целях, также поспособствует увеличению количества мошенничеств [13]. Становится все более совершенной технология «дипфейк» [14]. Теперь для компьютерного синтеза изображения или голоса не требуются большие массивы информации, достаточно лишь непродолжительной беседы, в результате которой нейросеть сгенерирует виртуальную копию человека, не только похожую на него внешне, но и имеющую те же ценности и предпочтения, что и он. А это, в свою очередь, уменьшит временные и финансовые затраты мошенников на создание дипфейков, существенно затруднит их распознавание и сделает киберпреступность если не более опасной, то более изощренной [15].

ЗАКЛЮЧЕНИЕ

Волна дистанционного мошенничества, захлестнувшая Россию в последние годы, несмотря на ряд профилактических мер, принятых государством, заставляет нас вновь уделять внимание данной проблеме. Сегодня в числе схем, которые используют злоумышленники для обмана граждан, особого внимания заслуживают: схема «FakeBoss» с переводом денежных средств на «безопасный счет»; имитация голоса родных и близких в аудиосообщениях; звонки по видеосвязи для идентификации клиентов банка по биометрии; звонки по видеосвязи якобы из правоохранительных органов и специальных служб. Появление и распространение трех последних сценариев обусловлены развитием технологии «дипфейк», которая становится всё более совершенной. Полагаем, что она по-прежнему будет использоваться в криминальных целях наряду с иными уже проверенными мошенниками средствами подготовки и реализации преступного замысла. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Колычева А.Н. Основные виды и способы осуществления преступной деятельности в сети Интернет // Современное общество и право. 2021. № 6 (55). С. 87-92.

2. Жданова О.В., Лабовская Ю.В., Дедюхина И.Ф. Финансовое мошенничество в современном мире // Государственная служба и кадры. 2020. № 4. С. 95-97.

3. Лабутин А.А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. № 2 (12). С. 50-55.

4. Алексеева А.П. Киберпреступность: насколько реальна угроза // Научно-методический электронный журнал «Концепт». 2017. № Т31. С. 76-80.

5. Алексеева А.П., Смагоринский Б.П., Третьяков В.И. Нейросети как инструмент работы органов внутренних дел: криминологический аспект // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 85-92.

6. Старостенко Н.И. Криминалистическое прогнозирование преступлений, совершаемых с использованием «deepfake»-технологий // Вестник Сибирского юридического института МВД России. 2023. № 2 (51). С. 187-192.

7. Бессонов А.А. Криминалистическая характеристика преступления // Пробелы в российском законодательстве. 2014. № 4. С. 171-173.

8. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.

9. Никитина И.А. Финансовое мошенничество в сети Интернет // Вестник Томского государственного университета. 2010. № 337. С. 122-124.

10. Киселев А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54-64.

[1] Мошенники начали использовать схему с «инкассацией» наличных // Совкомблог: сайт. 21.11.2024 // URL: https://journal.sovcombank.ru/news/moshenniki-nachali-ispolzovat-shemu-s-inkassatsiei-nalichnih (дата обращения: 25.11.2024).

11. Санина Л.В., Чепинога О.А., Ржепка Э.А., Палкин О.Ю. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения // Baikal Research Journal. 2021. Т. 12. № 2. С. 14.

12. Алексеева А.П. Перспективы развития уголовного законодательства в киберсфере // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: Сборник научных трудов по материалам II Всероссийской межвузовской научно-практической конференции. Вып. 2. Волгоград: ВА МВД России, 2017. С. 24-31.

13. Логинов М.П., Усова Н.В., Полубоярских Г.В., Антонова Е.А. Повышение угроз мошенничества при развитии рынка криптовалют // Балтийский экономический журнал. 2023. № 1 (41). С. 71-82.

14. Ефремова М.А., Русскевич Е.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 97-105.

15. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы // Уголовное законодательство: вчера, сегодня, завтра. Материалы ежегодной международной научно-практической конференции. СПб: СПбУ МВД России, 2024. С. 13-15.

REFERENCES

1. Kolycheva A.N. Osnovnyye vidy i sposoby osushchestvleniya prestupnoy deyatel'nosti v seti Internet // Sovremennoye obshchestvo i pravo. 2021. № 6 (55). S. 87-92.

2. Zhdanova O.V., Labovskaya Yu.V., Dedyukhina I.F. Finansovoye moshennichestvo v sovremennom mire // Gosudarstvennaya sluzhba i kadry. 2020. № 4. S. 95-97.

3. Labutin A.A. «Mobil'nyye» moshennichestva: osnovnyye sposoby sovershenia // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2013. № 2 (12). S. 50-55.

4. Alekseyeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». 2017. № T31. S. 76-80.

5. Alekseyeva A.P., Smagorinskiy B.P., Tret'yakov V.I. Neyroseti kak instrument raboty organov vnutrennikh del: kriminologicheskiy aspekt // Nauchnyy vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. 2023. № 3 (96). S. 85-92.

6. Starostenko N.I. Kriminalisticheskoye prognozirovaniye prestupleniy, sovershayemykh s ispol'zovaniyem «deepfake»-tekhnologiy // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. 2023. № 2 (51). S. 187-192.

7. Bessonov A.A. Kriminalisticheskaya kharakteristika prestupleniya // Probely v rossiyskom zakonodatel'stve. 2014. № 4. S. 171-173.

8. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.

9. Nikitina I.A. Finansovoye moshennichestvo v seti Internet // Vestnik Tomskogo gosudarstvennogo universiteta. 2010. № 337. S. 122-124.

10. Kiselev A.S. O neobkhodimosti pravovogo regulirovaniya v sfere iskusstvennogo intellekta: dipfeyk kak ugroza natsional'noy bezopasnosti // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Yurisprudentsiya. 2021. № 3. S. 54-64.

11. Sanina L.V., Chepinoga O.A., Rzhepka E.A., Palkin O.Yu. Destruktivnaya sotsial'naya inzheneriya kak ugroza ekonomicheskoy bezopasnosti: masshtaby yavleniya i mery predotvrashcheniya // Baikal Research Journal. 2021. T. 12. № 2. S. 14.

12. Alekseyeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov politsii k ispol'zovaniyu informatsionnykh tekhnologiy v bor'be s prestupnost'yu: Sbornik nauchnykh trudov po materialam II Vserossiyskoy mezhvuzovskoy nauchno-prakticheskoy konferentsii. Vyp. 2. Volgograd: VA MVD Rossii, 2017. S. 24-31.

13. Loginov M.P., Usova N.V., Poluboyarskikh G.V., Antonova Ye.A. Povysheniye ugroz moshennichestva pri razvitii rynka kriptovalyut // Baltiyskiy ekonomicheskiy zhurnal. 2023. № 1 (41). S. 71-82.

14. Yefremova M.A., Russkevich Ye.A. Dipfeyk (deepfake) i ugolovnyy zakon // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2024. T. 15. № 2 (56). S. 97-105.

15. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v sfere ustanovleniya ugolovnoy otvetstvennosti za nezakonnyye ispol'zovaniye i peredachu, sbor i khraneniye komp'yuternoy informatsii, soderzhashchey personal'nyye dannyye: problemy i perspektivy // Ugolovnoye zakonodatel'stvo: vchera, segodnya, zavtra. Materialy yezhegodnoy mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2024. S. 13-15.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Голятина С.М. Криминалистическое прогнозирование дистанционного мошенничества // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 4 (78). С. 75-80.