

Научная статья

УДК 343.9

Рубрика: Криминалистические исследования

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

Россия, 400075, г. Волгоград, ул. Историческая, 130.

Криминалистическое прогнозирование дистанционного мошенничества

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

АННОТАЦИЯ.

Введение. В настоящее время киберпреступность в целом и кибермошенничества в частности признаны национальной проблемой. Число этих преступлений растет из года в год, ущерб от них исчисляется миллиардами рублей, жертвами становятся все категории граждан: от несовершеннолетних до пенсионеров. Появление и развитие технологий искусственного интеллекта дали злоумышленникам новые возможности для совершения уголовно наказуемых деяний. Понимание тенденций развития киберпреступности позволит выработать стратегии борьбы с ней и оценить эффективность принимаемых сегодня мер.

Методы. В работе 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 изучения научной литературы по теме исследования автором сформулировано понятие криминалистического прогнозирования как научно обоснованного предвидения 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 автором исследована история развития киберпреступности в России, отмечены причины и условия, способствующие ее росту, составлен криминалистический прогноз развития ситуации в будущем. Выявлены тенденции дистанционного

мошенничества, намечены вероятные пути изменений мошеннических схем. Все это необходимо для разработки эффективной системы упреждающих мер, что сделает профилактику таких преступлений более действенной.

Svetlana Mikhailovna GOLYATINA

Candidate of Law Sciences,

ORCHID 0000-0001-6077-9827

Volgograd Academy of the Ministry of Internal Affairs of Russia (Volgograd),

Associate Professor of the Department of Criminology of the educational and scientific complex for preliminary investigation in the internal affairs bodies

sgoliatina@mvd.ru

Russia, 400075, Volgograd, st. Historical, 130.

Scientific article

UDC 343.9

Criminalistic forecasting remote fraud

KEYWORDS. Cybercrime, remote fraud, deepfake, forecast, forecast background, method of committing a crime.

ABSTRACT.

Introduction. Currently, cybercrime in general and cyberbullying in particular are recognized as a national problem. The number of these crimes is growing from year to year, the damage from them amounts to billions of rubles, and all categories of citizens are becoming victims: from minors to pensioners. The emergence and development of artificial intelligence technologies have given attackers new opportunities to commit criminal acts. Understanding trends in the development of cybercrime will allow us to develop strategies to combat it and assess the effectiveness of measures taken today.

Methods. The work used the dialectical method necessary for a complete and comprehensive study of phenomena, connections and contradictions between them, as well as description, logical methods (analysis and synthesis, induction and deduction), statistical method, methods of forensic forecasting.

Results. Based on the study of scientific literature on the subject of the study, the author formulated the concept of forensic forecasting as 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 of combating crime, technical and forensic tools used in the investigation of crimes, and forensic science in general. Guided by this definition, the author examines the history of the development of cybercrime in Russia, identifies the causes and conditions contributing to its growth, and makes a forensic forecast of the situation in the future. Trends in remote fraud have been identified, and possible ways of changing fraudulent schemes have been outlined.

All this is necessary to develop an effective system of preventive measures that will make the prevention of such crimes more effective.

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 тыс. киберпреступлений, что на 29,7 % больше, чем в 2022 году. Ущерб от действий злоумышленников составил 156 млрд руб.¹ Большая часть таких преступлений (53%) пришлась на мошенничества². С ними в 2023 году столкнулся 91 % россиян. С платежных карт преступникам удалось похитить 7,1 млрд руб., с банковских счетов – 4,6 млрд руб., через систему быстрых платежей – 3,3 млрд руб., с электронных кошельков – 105,2 млн руб.³ В число популярных технологий обмана граждан входили схема с «безопасным» счетом [1, с. 87-92], обещания сверхприбыли на бирже [2, с. 95-97], финансовые пирамиды [3, с. 50-55], фишинг [4, с. 76-80] и др. Заместитель председателя правления Сбера С. Кузнецов по этому поводу говорил: «Прежде всего, наиболее актуальными и опасными 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»⁴. Всего в 2023 году злоумышленники провели

¹ См.: За пять лет число киберпреступлений увеличилось более чем вдвое. URL: <https://rg.ru/2024/09/25/policiia-v-seti.html> (дата обращения: 01.11.2024).

² См.: Россия – одна из стран с очень высоким уровнем киберугроз. Но до полиции доходит меньше половины преступлений и только четверть из них раскрывают. URL: <https://tochno.st/materials/rossiia-odna-iz-stran-s-ocen-vysokim-urovнем-kiberugroz-no-do-policii-dohodit-mense-poloviny-prestuplenii-i-tolko-cetvert-iz-nix-raskryvaiut>(дата обращения: 01.11.2024).

³ См.: Павлова М. 8 фактов о мошенничестве в России: от финансовых пирамид до кибератак. URL: <https://journal.tinkoff.ru/short/ne-obmanuly/> (дата обращения: 01.11.2024).

⁴Зампред Сбера рассказал о воздействии мошенников на эмоции людей. URL: <https://lenta.ru/news/2024/09/04/rasskazal/> (дата обращения: 01.11.2024).

1,17 млн успешных операций. По данным Центрального банка России, причина сложившейся ситуации состоит в адресных и подготовленных атаках¹, а также в том, 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, с. 85-92]. 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 будут фиксироваться в ближайшее время? Какие трансформации ждут киберпреступность? Каковы тенденции ее развития? Ответы на эти вопросы поможет 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 составил диалектический метод, необходимый для полного и всестороннего изучения явлений, связей и противоречий между ними, а также совокупность обще- и частнонаучных методов: описание – для характеристики материала, логические методы (анализ и

¹ См.: Корочкина А. Кибермошенники украли почти 16 млрд руб. у россиян в 2023 г. URL: <https://www.forbes.ru/finansy/506131-kibermosenniki-ukrali-pochti-16-mlrd-rublej-u-rossian-v-2023-godu> (дата обращения: 01.11.2024).

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 г., 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 видов¹. Спустя время это предположение получило развитие в трудах Р. С. Белкина, который выделил объекты прогнозирования: 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: 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

¹Голунский С. А., Шавер Б. М. Криминалистика. Методика расследования отдельных видов преступлений: учебник / под ред. А. Я. Вышинского. М.:Юрид. изд-во НКЮ СССР, 1939. 372 с.

²Белкин Р. С. Ленинская теория отражения и методологические проблемы советской криминалистики: учебное пособие по курсу советской криминалистики. М.: Высш. шк. МВД СССР, 1970. 130 с.

³Зуйков Г. Г. Криминалистическое учение о способе совершения преступления: автореф. дис. ... д-ра юрид. наук. М., 1970. 30 с. – С. 10.

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 совершения дистанционных мошенничеств (точнее, схемах), рассмотрим данный вид преступных посягательств с позиции криминалистического прогноза. Обычно он 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 гг. и представляла собой попытки взлома операционных систем и получения доступа к конфиденциальной информации [8, с. 27-34]. Затем злоумышленники начали 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 1990-е гг., 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 столь стремительный рост (см. рис. 1). При этом важно отметить, что на протяжении многих лет большую часть киберпреступлений составляют именно кибермошенничества.

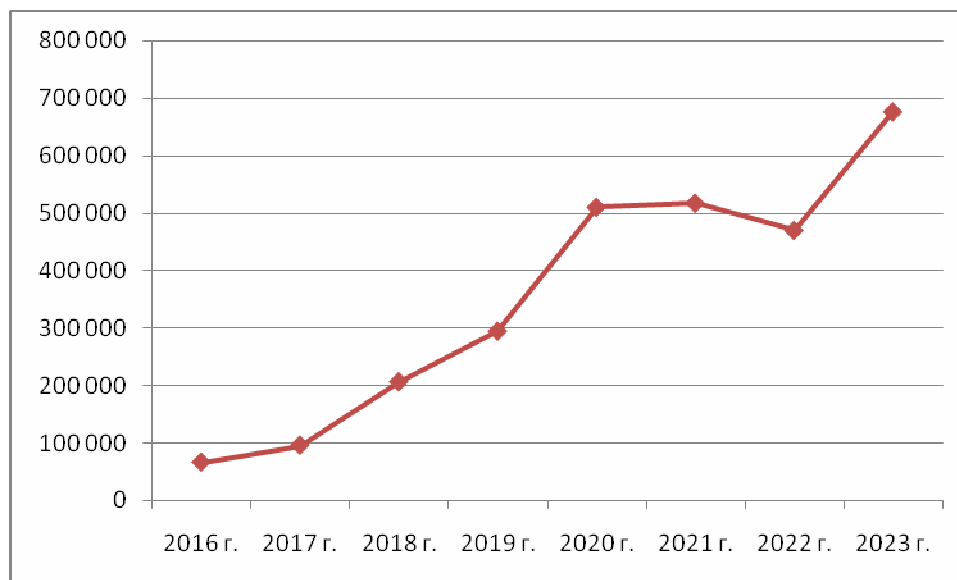


Рис. 1. Число киберпреступлений, зарегистрированных в России в 2016–2023 гг. (по данным МВД России)¹

Второй этап криминалистического прогнозирования называется *прогноznым 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 сотрудники Сбера: «...Мы имеем мировое лидерство с точки зрения потерь, с точки зрения масштабов бедствия от телефонного мошенничества»². По словам 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»³. Популярными схемами мошенничества являются:

– схема «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 участии в

¹Состояние преступности: статистика и аналитика // МВД России: сайт. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 25.11.2024).

² См.: Сбербанк заявил о лидерстве России по масштабам ущерба от телефонных мошенников. URL: <https://www.kommersant.ru/doc/6747796> (дата обращения: 01.11.2024).

³ Романова Т. В Сбере назвали критической ситуацией с телефонным мошенничеством. URL: <https://lenta.ru/news/2024/06/04/kriticheskoy/> (дата обращения: 25.11.2024).

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 сумму на указанный мошенниками счет и после этого осознает, что стал жертвой обмана [9, с. 122-124];

– имитация голоса родных и близких в аудиосообщениях (голоса генерируются с помощью технологии «дипфейк») [9, с. 50-55];

– звонки по видеосвязи для идентификации клиентов банка по биометрии [10, с. 54-64];

– 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), который предъявил служебное удостоверение и убедил женщину перевести 500 тыс. руб. 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 практически 1 млн руб.¹ От жительницы г. Барнаула М. ее родственникам, друзьям и знакомым стали приходиться голосовые и видеосообщения с просьбой одолжить ей денег. Как оказалось позже, когда на счет злоумышленников уже были отправлены совокупно 100 тыс. руб., аккаунт М. был взломан, а ее голос и внешность – результат работы нейросети². Жительница г. Зуевки Кировской области перевела на счет злоумышленников

¹См.: Жительница Чебоксар перевела мошенникам почти миллион рублей, поверив в дипфейк. URL: <https://www.kommersant.ru/doc/7299409> (дата обращения: 02.11.2024).

²См.: Усик А. «Взломать могут любого». От имени жительницы Барнаула разослали дипфейки с просьбой занять денег. URL: <https://www.alt.kp.ru/daily/27640.5/4990570/> (дата обращения: 02.11.2024).

300 000 руб. 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 Роберт Дауни-младший и представился полицейским, попытался выманить деньги у женщины, но потерпел неудачу¹. Отметим, что с начала 2024 г. число преступных схем с использованием дипфейков выросло в 30 раз².

Обеспокоенность вызывают не только дипфейки, но и появляющиеся схемы мошенничества с цифровым рублем (хотя в настоящее время он запущен в тестовом режиме). РИА «Новости» со ссылкой на члена комитета Государственной Думы Федерального Собрания Российской Федерации по информполитике А. Немкина пишут, 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...»³, – т. е. схемы мошенничества здесь, в общем, такие же, как с безналичными денежными средствами.

Кроме того, после внесения изменений в Федеральный закон «О национальной платежной системе» № 161-ФЗ от 27 июня 2011 г. (внедрение «периода охлаждения», отключение каналов дистанционного банковского обслуживания «дропам») мошенники начали убеждать россиян снимать деньги со

¹ См.: Джабборов Д. Мошенник с лицом Роберта Дауни-младшего попытался украсть деньги кировчанина. URL: <https://www.gazeta.ru/tech/news/2024/03/22/22608199.shtml> (дата обращения: 02.11.2024).

²Состояние преступности: статистика и аналитика // МВД России: сайт. URL:<https://мвд.рф/dejatelnost/statistics>(дата обращения: 25.11.2024).

³ В России выстроены первые схемы мошенничества с цифровым рублем. URL: https://www.cnews.ru/news/top/2024-07-04_v_rossii_poyavilis_pervye (дата обращения: 25.11.2024).

счетов и передавать их «инкассаторам», которые якобы перевезут их в другой банк на хранение (вместо перевода на «безопасный» счет). Такая схема позволяет злоумышленникам обойти антифрод-проверки, следовательно, набирает популярность [12, с. 24-31]. По информации сервиса DLBI, на нее уже приходится около 80 % всех случаев хищений¹. Из сказанного можно сделать вывод о том, что киберпреступность продолжает развиваться и адаптироваться к новым вызовам и технологиям.

Третий этап криминалистического прогнозирования – проспекция, где происходит разработка прогнозов на основе диагноза. С учетом статистических данных о состоянии киберпреступности в стране, схем мошенничества, которые приспособляются 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 «Центробанка России» с рекомендациями перевести денежные средства на «безопасный» счет или отдать их «инкассаторам» будут активно использоваться злоумышленниками, так как они просты в исполнении и вот уже на протяжении нескольких лет, несмотря на профилактическую работу, приносят преступникам самую большую прибыль. Появление и стремительное развитие искусственного интеллекта и других инноваций, которые киберпреступники могут использовать в своих целях, также способствует увеличению количества мошенничеств [13, с. 71-82]. Становится все более совершенной технология «дипфейк» [14, с. 97-105]. Теперь для ее создания не требуются большие массивы информации, достаточно лишь непродолжительной беседы, в результате которой нейросеть генерирует виртуальную копию человека, не только похожую внешне, но и имеющую те же ценности и предпочтения, что и оригинал, а это, в свою очередь, уменьшит

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

временные и финансовые затраты мошенников на создание дипфейков, существенно затруднит их распознавание и сделает киберпреступность если не более опасной, то более изощренной [15, с. 13-15].

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 более совершенной и, полагаем, по-прежнему будет использоваться в криминальных целях наряду с иными уже проверенными мошенниками схемами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

2. Жданова, О. В. Финансовое мошенничество в современном мире / О. В. Жданова, Ю. В. Лабовская, И. Ф. Дедюхина // Государственная служба и кадры. – 2020. – № 4. – С. 95-97. – DOI 10.24411/2312-0444-2020-10194. – EDNMUTNXR.

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

4. Алексеева, А. П. Киберпреступность: насколько реальна угроза / А. П. Алексеева // Научно-методический электронный журнал "Концепт". – 2017. – № Т31. – С. 76-80. – EDNYPIB.

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

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

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

10. Киселев, А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А. С. Киселев // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – № 3. – С. 54-64. – DOI 10.18384/2310-6794-2021-3-54-64. – EDNAHJBNN.

11. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения / Л. В. Санина, О. А. Чепинога, Э. А. Ржепка, О. Ю. Палкин // BaikalResearchJournal. – 2021. – Т. 12, № 2. – DOI 10.17150/2411-6262.2021.12(2).14. – EDNGREEFK.

12. Алексеева, А. П. Перспективы развития уголовного законодательства в киберсфере / А. П. Алексеева // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: Сборник научных трудов по материалам II Всероссийской межвузовской научно-практической конференции, Волгоград, 06 декабря 2016 года. Том Выпуск 2. – Волгоград: Волгоградская академия Министерства внутренних дел Российской Федерации, 2017. – С. 24-31. – EDNCJZXYJ.

13. Повышение угроз мошенничества при развитии рынка криптовалют / М. П. Логинов, Н. В. Усова, Г. В. Полубоярских, Е. А. Антонова // Балтийский экономический журнал. – 2023. – № 1(41). – С. 71-82. – DOI 10.46845/2073-3364-2023-0-1-71-82. – EDNWNWDBM.

14. Ефремова, М. А. Дипфейк (deepfake) и уголовный закон / М. А. Ефремова, Е. А. Русскевич // Вестник Казанского юридического института МВД России. – 2024. – Т. 15, № 2(56). – С. 97-105. – DOI 10.37973/VESTNIKKUI-2024-56-13. – EDNLXAWLM.

15. Алексеева, А. П. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы / А. П. Алексеева, Т. В. Анисимова // Уголовное законодательство: вчера, сегодня, завтра : Материалы ежегодной международной научно-практической конференции, Санкт-Петербург, 07–08 июня 2024 года. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2024. – С. 13-15. – EDNNFQDPB.

REFERENCES

1. Kolycheva, A. N. Osnovnye vidy i sposoby osushchestvleniya prestupnoj deyatel'nosti v seti Internet / A. N. Kolycheva // Sovremennoe obshchestvo i pravo. – 2021. – № 6(55). – S. 87-92. – EDNUZKWEU.

2. ZHdanova, O. V. Finansovoe moshennichestvo v sovremennom mire / O. V. ZHdanova, YU. V. Labovskaya, I. F. Dedyuhina // Gosudarstvennaya sluzhba i kadry. – 2020. – № 4. – S. 95-97. – DOI 10.24411/2312-0444-2020-10194. – EDNMUTNXR.
3. Labutin, A. A. "Mobil'nye" moshennichestva: osnovnye sposoby soversheniya / A. A. Labutin // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. – 2013. – № 2(12). – S. 50-55. – EDNQJBGTD.
4. Alekseeva, A. P. Kiberprestupnost': naskol'ko real'na ugroza / A. P. Alekseeva // Nauchno-metodicheskij elektronnyj zhurnal "Koncept". – 2017. – № T31. – S. 76-80. – EDNYPISIB.
5. Alekseeva, A. P. Nejroseti kak instrument raboty organov vnutrennih del: kriminologicheskij aspekt / A. P. Alekseeva, B. P. Smagorinskij, V. I. Tret'yakov // Nauchnyj vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. – 2023. – № 3(96). – S. 85-92. – EDNNQACBX.
6. Starostenko N. I. Kriminalisticheskoe prognozirovanie prestuplenij, sovershaemyh s ispol'zovaniem «deepfake»-tekhnologij // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. 2023. № 2 (51). S. 187–192.
7. Bessonov A. A. Kriminalisticheskaya harakteristika prestupleniya // Probely v rossijskom zakonodatel'stve. 2014. № 4. S. 171–173.
8. Alekseeva, A. P. Kiberprestupnost': osnovnye cherty i formy proyavleniya / A. P. Alekseeva, O. N. Nichugovskaya // Prestupnost' v sfere informacionnyh i telekommunikacionnyh tekhnologij: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenij. – 2017. – № 1. – S. 27-34. – EDNZGSRDF.
9. Nikitina, I. A. Finansovoe moshennichestvo v seti Internet / I. A. Nikitina // Vestnik Tomskogo gosudarstvennogo universiteta. – 2010. – № 337. – S. 122-124. – EDNNBVEMN.
10. Kiselev, A. S. O neobhodimosti pravovogo regulirovaniya v sfere iskusstvennogo intellekta: dipfejk kak ugroza nacional'noj bezopasnosti / A. S. Kiselev // Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya:

YUrisprudenciya. – 2021. – № 3. – S. 54-64. – DOI 10.18384/2310-6794-2021-3-54-64. – EDNAHJBNH.

11. Destruktivnaya social'naya inzheneriya kak ugroza ekonomicheskoy bezopasnosti: masshtaby yavleniya i mery predotvrashcheniya / L. V. Sanina, O. A. CHepinoga, E. A. Rzhepka, O. YU. Palkin // *BaikalResearchJournal*. – 2021. – T. 12, № 2. – DOI 10.17150/2411-6262.2021.12(2).14. – EDNGREEFK.

12. Alekseeva, A. P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere / A. P. Alekseeva // *Podgotovka sotrudnikov policii k ispol'zovaniyu informacionnyh tekhnologij v bor'be s prestupnost'yu: Sbornik nauchnyh trudov po materialam II Vserossijskoj mezhvuzovskoj nauchno-prakticheskoy konferencii, Volgograd, 06 dekabrya 2016 goda. Tom Vypusk 2.* – Volgograd: Volgogradskaya akademiya Ministerstva vnutrennih del Rossijskoj Federacii, 2017. – S. 24-31. – EDNCJZXYJ.

13. Povyshenie ugroz moshennichestva pri razvitii rynka kriptovalyut / M. P. Loginov, N. V. Usova, G. V. Poluboyarskih, E. A. Antonova // *Baltijskij ekonomicheskij zhurnal*. – 2023. – № 1(41). – S. 71-82. – DOI 10.46845/2073-3364-2023-0-1-71-82. – EDNWNWDBM.

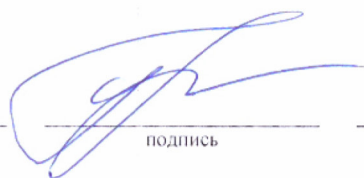
14. Efremova, M. A. Dipfejk (deepfake) i ugolovnyj zakon / M. A. Efremova, E. A. Russkevich // *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*. – 2024. – T. 15, № 2(56). – S. 97-105. – DOI 10.37973/VESTNIKKUI-2024-56-13. – EDNLXAWLM.

15. Alekseeva, A. P. Zakonodatel'nye iniciativy v sfere ustanovleniya ugolovnoj otvetstvennosti za nezakonnye ispol'zovanie i peredachu, sbor i hranenie komp'yuternoj informacii, sodержashchej personal'nye dannye: problemy i perspektivy / A. P. Alekseeva, T. V. Anisimova // *Ugolovnoe zakonodatel'stvo: vchera, segodnya, zavtra : Materialy ezhegodnoj mezhdunarodnoj nauchno-prakticheskoy konferencii, Sankt-Peterburg, 07–08 iyunya 2024 goda.* – Sankt-Peterburg: Sankt-Peterburgskij universitet MVD Rossii, 2024. – S. 13-15. – EDNNFQDPB.

Представленный материал ранее не публиковался в настоящее время не аходится на рассмотрении на предмет публикации в других изданиях. Заявляю об отсутствии конфликта интересов, связанного с публикацией данной статьи в журнале «Вестник Калининградского филиала Санкт-Петербургского университета МВД России». Разрешаю размещение полнотекстовой версии статьи, а также её частей в открытом доступе в сети Интернет, а также на официальных каналах журнала в социальных сетях. При создании статьи не использовались возможности искусственного интеллекта.

Голятина С.М.

Ф.И.О. субъекта персональных данных



подпись

11.11.2024

дата