Научная статья
УДК 343.98
https://doi.org/10.36511/2078-5356-2023-1-70-76

Об использовании технологии *“Deepfake”* в оперативно-розыскной деятельности

Батоев Владимир Батоевич
Научно-производственное объединение «Специальная техника и связь» МВД России, Москва, Россия, vbatoev@mail.ru

Аннотация. В статье обозначен потенциал и дана оценка перспективе использования в оперативно-розыскной деятельности новой информационной технологии *“Deepfake”*, основанной на искусственном интеллекте и генеративно-состязательных нейросетях. Обозначен ряд проблемных вопросов, требующих разрешения для эффективного применения указанной технологии при решении задач оперативно-розыскной деятельности. Акцентировано внимание на необходимости использования технологии *“Deepfake”* в рамках дезинформирования преступной среды. Синтетический медиаконтент в современных условиях способен обеспечить решение оперативно-розыскных задач различной направленности, особым образом подчеркивая перспективность применения технологии *“Deepfake”* в деятельности оперативных подразделений в качестве специфического метода, ранее не изученного в оперативно-розыскной теории и не использовавшегося в оперативно-розыскной практике. В условиях необратимой цифровизации всех сфер общественных отношений обозначена необходимость скорейшего перехода организации и тактики оперативно-розыскной деятельности в новую фазу, где роль постоянно совершенствующихся информационных технологий в оперативно-розыскной деятельности должна носить приоритетный характер.

Ключевые слова: информационные технологии, оперативно-розыскная деятельность, искусственный интеллект, противодействие преступности, генеративно-состязательные нейросети, дипфейк, *“Deepfake”*, дезинформация, манипулирование

Для цитирования: Батоев В. Б. Об использовании технологии *“Deepfake”* в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 70—76. https://doi.org/10.36511/2078-5356-2023-1-70-76.

Original article

About the use of “Deepfake” technology in operational investigative activities

Vladimir B. Batoev
Research and Production Association “Special Equipment and Communications” of the Ministry of Internal Affairs of Russia, Moscow, Russian Federation, vbatoev@mail.ru

Abstract. The article identifies the potential and assesses the prospect of using the new information technology “Deepfake” based on artificial intelligence and generative-adversarial neural networks in operational investigative activities. A number of problematic issues have been identified that require resolution for the effective use of this technology in solving the tasks of operational investigative activities. Attention is focused on the need to use the “Deepfake” technology in the framework of misinformation of the criminal environment. Synthetic media content in modern conditions is able to provide a solution to operational-investigative tasks of various directions, emphasizing in a special way the prospects of using the “Deepfake” technology in the activities of operational units as a specific method not previously studied in operational-investigative theory and not used in operational-investigative practice. In the conditions of irreversible digitalization of all spheres of public relations, the need for an early transition of the organization and tactics of operational investigative activities into a new phase is indicated, where the role of constantly improving information technologies in operational investigative activities should be a priority.

Keywords: information technologies, operational investigative activity, artificial intelligence, crime prevention, generative-adversarial neural networks, deepfake, “Deepfake”, deinformation, manipulation

For citation: Batoev V. B. On the use of “Deepfake” technology in operational investigative activities. *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 1, pp. 70—76. https://doi.org/10.36511/2078-5356-2023-1-70-76.

Интенсивное развитие технической мысли и последние достижения науки и техники в сфере цифровых технологий, а также нарастающие возможности технологий искусственного интеллекта, машинного обучения, больших данных существенно облегчили жизнь человека и заметно упростили вопросы организации общественных процессов.

На этом фоне особо выделяются постоянно совершенствующиеся механизмы создания, обработки и хранения цифровой информации, используемые как в социально-полезных и криминальных целях в целом, так и в рамках манипулирования индивидуальным и общественным сознанием, в частности.

Общество столкнулось с невиданными ранее темпами развития технологий по созданию реалистичных несуществующих в природе видеоизображений и аудиосообщений посредством использования искусственного интеллекта, машинного обучения, нейронных сетей посредством наложения видео и фотоизображений, аудиосообщений друг на друга в развлекательных видеороликах, кино, рекламе и др. [15, с. 63]. Такое представилось возможным благодаря развитию современных технологий в данном направлении, которые сделали весьма доступной возможность для любого человека создавать качественные фотовидеоизображения, аудиосообщения с высокой степенью правдоподобности, что в ряде случаев воспринимается рядовыми гражданами в качестве фактов, событий и явлений из реальной действительности.

Одновременно с этим определенную неоднозначность в оценке эффективности таких новшеств привнесли технологии создания поддельных «синтетических» видео, фотоизображений и аудиосообщений — *“Deepfake”*, под которыми предлагаем понимать совокупность методов соединения или объединения, ранее разрозненных видеофотоизображений и аудиосообщений посредством использования технологии генеративно-состязательных нейросетей в единое поддельное целое.

С этимологической стороны термин *“Deepfake”* представляет собой комбинацию слов *“deep learning”* («глубокое обучение») и слова *“fake”* (подделка), образуя дословно «подделка на глубоком уровне». Технология *“Deepfake”* была разработана в 2014 году студентом Стэндфордского университета Яном Гудфеллоу. С тех пор различные компании разработчики активно развивают и совершенствуют нейросети, составляющие основу *“Deepfake”*, и предлагают широкий спектр инструментария по созданию «поддельного» контента. Как следствие, приходится констатировать факт, что в настоящее время обычный пользователь имеет возможность посредством использования приложения в мобильном устройстве или сотовом телефоне, без применения каких-либо специальных познаний и дополнительных технических средств создавать фото, видеоизображения или аудиосообщения различного содержания и целевой направленности.

Такая шаговая доступность, многообразие приложений и простота в создании дипфейков привлекла внимание криминалитета. Первым ярким примером использования данной технологии в противоправных целях стало распространение в 2017 году в сети «Интернет» роликов порнографического характера с лицами известных голливудских актрис [1]. Далее по мере развития и распространения технологии поддельные фото, видеоизображения и аудиосообщения также стали активно использоваться при совершении таких преступлений, как клевета, мошенничество, вымогательство, незаконные изготовление и оборот порнографических материалов или предметов и др. [2]. Более того, использование дипфейков нашло применение при преследовании и унижении чести и достоинства человека, при подделке документов, фальсификации электронных видов доказательств, распространении дезинформации и манипулировании общественным мнением, поддержке нарративов экстремистских и террористических групп, разжигании социальных и политических волнений, при противодействии правоохранительным органам, когда используется специальный вброс дезинформации в сеть «Интернет» в виде изображений лица, якобы причастного к совершению преступления, при компрометации деятельности государственных органов и др.

Подобные вызовы сформировали неопределенность государства в решении вопросов правовой оценки и принятия мер соответствующего реагирования. Изучение юридической литературы показывает, что технологии *“Deepfake”*, используемые в криминальных целях, не

урегулированы нормами уголовного законодательства, а аспекты уголовно-правовой квалификации сводятся к точке зрения о необходимости введения уголовной ответственности за создание и распространение дипфейков в криминальных целях, а также признания использования дипфейков в противоправных целях в качестве обстоятельства, отягчающего преступность деяния [3—5]. Сравнение данных точек зрения позволяет заключить, что вопросы уголовно-правовой квалификации использования технологии *"Deepfake"* в преступных целях необходимо разрешить уже сейчас, в том числе с рассмотрением таких вопросов сквозь призму административной преюдиции.

Здесь же добавим, что одним из возможных выходов в разрешении вопросов уголовно-правовой квалификации использования дипфейков в противоправных целях может послужить изучение передовых эффективных зарубежных практик. Так, изучение международного опыта показывает, что в США на законодательном уровне в отдельных штатах [6] было запрещено использование дипфейковых фото- и видеоизображений, аудиосообщений в течение 60 суток до выборов в законодательные и представительные органы [7, с. 380—381], в Китайской Народной Республике создание и распространение дипфейков признается уголовно наказуемым деянием [8] и др.

Полагаем, что игнорирование потенциальной угрозы от бесконтрольного применения данной технологии в противоправных целях может привести к неуправляемой ситуации, когда использование дипфейков выступит инструментом совершения различных видов преступлений. Подобная криминальная активность в деле использования дипфейков в преступной деятельности требует со стороны правоохранительных органов взвешенной оценки складывающейся ситуации, выработку методов и средств их выявления, повышения уровня технической оснащенности и квалификации сотрудников правоохранительных органов, что непременно предопределяет необходимость проведения фундаментальных научных исследований. Взятие данной ситуации под должный контроль со стороны государства подразумевает разработку действенного законодательства по всем вопросам правового регулирования использования дипфейков, где законодатель в первую очередь должен учесть потребности правоохранительных органов.

Рассуждая о необходимости разработки государством дорожной карты по взятию под должный контроль использование технологии "Deepfake", считаем необходимым обратить внимание на следующее.

С учетом того, что технология *"Deepfake"* получила широкую востребованность у общественности, а также активно используется в противоправной деятельности считаем целесообразным рассмотреть вопрос использования технологии *"Deepfake"* при решении оперативно-розыскных задач.

Оперативно-розыскная деятельность с сочетанием ее гласных и негласных начал выступает именно той сферой общественных отношений, где технологии *"Deepfake"* могли бы оказаться социально полезными с точки зрения их использования при решении задач борьбы с преступностью.

Так, дипфейковое фотовидеоизображение или аудиосообщение с поддельным образом или голосом можно было бы использовать в различных оперативно-розыскных ситуациях: при установлении обстоятельств совершения преступления; при определении роли в преступном событии каждого из участников преступной группы и выявлении новых участников; разобщении группы; при использовании легендированных объектов и др. В данном случае мы ведем речь именно о фотовидеоизображении и аудиосообщении дезориентирующего характера.

Нельзя забывать и то, что в соответствии с требованиями уголовно-процессуального законодательства использование доказательств, полученных на основе использования фото, видеоизображений или аудиосообщений с поддельным образом или голосом могут не быть признаны допустимыми, что в принципе исключает законную возможность использования дипфейков в целях получения информации, имеющей доказательственное значение.

Однако полагаем, что спектр оперативно-розыскных задач борьбы с преступностью довольно обширен, и в ряде случаев фотовидеоизображения или аудиосообщения с поддельным образом или голосом вполне можно использовать в целях дезинформирования криминальной среды. Иными словами, использовать дипфейки в качестве инструмента информационно-психологического воздействия на отдельный объект оперативной заинтересованности либо на группу лиц криминальной направленности.

Как отмечают Е. А. Михеев и Т. А. Нестик, дезинформация — это процесс манипулирования информацией: введение кого-либо в заблуждение путем предоставления неполной

информации или полной, но уже не нужной информации, искажения контекста, искажения части информации. При этом ими же предлагается под манипуляцией в психологии понимать вид психологического воздействия, при котором мастерство манипулятора используется для скрытого внедрения в психику адресата целей, желаний, намерений, отношений или установок, не совпадающих с теми, которые имеются у адресата в данный момент; психологическое воздействие, нацеленное на изменение направления активности другого человека, выполненное настолько искусно, что остается незамеченным им; психологическое воздействие, направленное на неявное побуждение другого к совершению определенных манипулятором действий; искусное побуждение другого к достижению (преследованию) косвенно вложенной манипулятором цели [9, с. 6—7].

Думается, что с оперативно-розыскной точки зрения именно преимущественно негласный характер деятельности сотрудников оперативных подразделений обусловливает необходимость использования информационно-психологического воздействия посредством дезинформации объектов оперативной заинтересованности, которую, по мнению Е. С. Дубоносова, можно условно разделить по объему — на полную и частичную, по масштабу — локальную и выборочную, по характеру воздействия на лиц, представляющую оперативный интерес — отвлекающую и побуждающую, и реализовать посредством использования средств массовой информации, средств межличностной неформальной коммуникации (слухи, сплетни и др.) и лиц, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность [10, с. 30].

Обращает на себя внимание отсутствие законодательного запрета на действия субъектов оперативно-розыскной деятельности по созданию и использованию дипфейков, что подразумевает проработку данного вопроса и введения возможности использования дипфейков при осуществлении оперативно-розыскной деятельности. В этой связи можно предположить возможным внесение в нормы оперативно-розыскного законодательства положения, предоставляющие законные основания для использования технологии *“Deepfake”* при решении задач оперативно-розыскной деятельности, по аналогии с нормой, разрешающей создание легендированных предприятий, учреждений, организаций и подразделений, создание и функционирование которых по своему смыслу в какой-то части схоже с предназначением дипфейков в частности, и дезинформирования объектов оперативной заинтересованности в целом. Полагаем, что подобная инициатива заслуживает внимания и практической реализации. Для этого в первую очередь необходимо разработать правовую основу использования технологии “Deepfake” с неукоснительным соблюдением прав и свобод человека и гражданина, законодательства при осуществлении оперативно-розыскной деятельности, в соотношении с вопросами провокации и фальсификации результатов оперативно-розыскной деятельности [11—18]. Здесь же обратим внимание, что источникам законодательной инициативы важно опираться на нормы основного закона Российской Федерации, который закрепляет обязанность государства признавать, соблюдать и защищать права и свободы человека и гражданина, и, одновременно, предоставляет возможность их ограничивать компетентным органам в установленном законом порядке в соразмерной мере в целях защиты прав и законных интересов других лиц [19, с. 4].

С учетом современных цифровых реалий и прогнозирования дальнейшего развития инженерной мысли по искомому вопросу можно заключить, что технология *“Deepfake”* наряду с иными внедренными технологиями, используемыми при решении оперативно-розыскных задач (распознавание лиц, геопозиционирование, биллинг, мониторинг сети «Интернет» и др.) станет необходимым атрибутом в имеющемся арсенале средств оперативно-розыскной деятельности. В оперативно-розыскной практике сформировался определенный опыт осуществления дезинформирования при решении задач борьбы с преступностью [20—22], однако дипфейки ранее не использовались в оперативно-розыскных целях. В связи с этим считаем вполне обоснованной необходимость создания соответствующих базовых технологических условий, организационной, тактической, правовой, кадровой и материально-технической основы для возможности использования технологии *“Deepfake”* при решении задач оперативно-розыскной деятельности, потенциал которой в условиях тотальной цифровизации трудно переоценить.

Таким образом, в условиях цифровой трансформации общественных процессов технологии создания синтетических медиа и диджитал-дезинформирования являются одними из самых многофункциональных по линии

применения. Примеры практики свидетельствуют, что наряду с социально-полезными целями создания синтезированных фото, видеоизображений и аудиосообщений в вопросах использования технологии *"Deepfake"* заметно преобладает над ними и нашло применение в вопросах манипулирования общественным мнением и дезинформирования отдельных лиц или социальных групп в криминальных целях. В связи с этим приходится констатировать наличие потенциальной угрозы для человека, общества и государства, в том числе в силу протекающих процессов качественного совершенствования данной технологии и повышения уровня доступности инструментария по созданию поддельных фото, видео и аудиообразов для широкого круга пользователей.

Стремительное развитие инфраструктурных и технических решений в данном направлении свидетельствует о наличии противостояния между технологиями по созданию дипфейков и их обнаружению на основе использования искусственного интеллекта, машинного обучения и нейронных сетей. Оперативно-розыскной теории и практике важно создать необходимую основу и совокупность сил, средств и методов как создания и использования дипфейков в оперативно-розыскных целях, так и их распознании. В настоящее время существует потребность в проведении научных исследований, посвященных вопросам использования дипфейков сквозь оперативно-розыскную призму, с выработкой научно обоснованных предложений и рекомендаций и обеспечением должного уровня методической обеспеченности по данным вопросам деятельности оперативных подразделений. Полагаем, что обозначенные ранее направления совершенствования оперативно-розыскной деятельности посредством использования технологии *"Deepfake"* можно отнести к числу приоритетных, где наступательность в части выбора новых эффективных средств противодействия преступности уже диктуется уровнем технологического противостояния преступности. Думается, что непринятие во внимание потенциала использования технологии *"Deepfake"* как в положительных, так и отрицательных целях может привести к созданию ситуации, при которой утрата опережающего характера организации оперативно-розыскной деятельности по борьбе с преступностью чревата проявлениями негативных последствий, что возможно предотвратить своевременным всесторонним изучением технических новинок и их практической реализацией.

Список источников

1. Человек с другим лицом: Что такое дипфейк и чем он опасен? URL: https://www.5-tv.ru/tabloid/306975/dipfejki-cto-eto-kak-rabotaet-icem-opasno/ (дата обращения: 25.12.2022).

2. Криминальная жизнь дипфейков. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov (дата обращения: 25.12.2022).

3. Грешнова Н. А., Ситник В. Н. Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake)) // Вестник Саратовской государственной юридической академии. 2022. № 5 (148). С. 182—189.

4. Данилова В. А., Левкин Д. М. Правовые аспекты регулирования "Deepfake" технологии в России // Право и государство: теория и практика. 2022. № 7 (211). С. 88—91.

5. Перина А. С. К вопросу о квалификации дипфейков: сборник материалов международной студенческой и научной конференции. Красноярск: СибЮИ МВД России, 2022. Вып. 24. С. 331—333.

6. Dent S. California cracks down on political and pornographic deepfakes. URL: https://www.engadget.com/2019-10-07-california-deepfake-pornography-politics.html (дата обращения: 22.12.2022).

7. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. № 4. С. 379—386.

8. В Китае ввели уголовное наказание за публикацию дипфейков без пояснений. URL: https://rtvi.com/news/v-kitae-vveli-ugolovnoe-nakazanie-za-publikatsiyu-dipfeykov-bez-poyasneniy/ (дата обращения: 25.12.2022).

9. Михеев Е. А., Нестик Т. А. Дезинформация в социальных сетях: состояние и перспективы психологических исследований // Социальная психология и общество. 2018. Т. 9. № 2. С. 5—20.

10. Дубоносов Е.С. Дезинформация криминальной среды при осуществлении оперативно-розыскной деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 2. С. 27—33.

11. Бердников В. Л. Субъективная сторона преступления, предусмотренного статьей 303 УК РФ // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2022. № 1 (100). С. 87—97.

12. Бурмистрова А. А. Правомерное оперативно-розыскное мероприятие «Ловушка» в правоприменительной практике Соединенных Штатов Америки и критерии его отграничения от провокации преступления // Сибирский антропологический журнал. 2022. Т. 6. № 3. С. 105—110.

13. Кокурин Г. А. О некоторых способах фальсификации результатов оперативно-розыскной деятельности // Российское право: образование, практика, наука. 2022. № 1. С. 75—80.

14. Сафонов А. Ю. Способы совершения преступлений по уголовным делам о фальсификации доказательств и (или) результатов ОРД // Алтайский юридический вестник. 2017. № 4. С. 122—127.

15. Семенцов В. А. Провокация преступления в оперативно-розыскной деятельности // Союз криминалистов и криминологов. 2020. № 4. С. 45—53.

16. Сущенко С. А. Проблема допустимости доказательств, полученных на основе оперативно-розыскной деятельности в результате провокации, в России и зарубежных странах: некоторые сравнительно-правовые аспекты // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3 (92). С. 228—234.

17. Шашин Д. Г. Оперативно-розыскные мероприятия и провокация: законность санкционирования и активных действий // Материалы Всероссийского научно-практического семинара. Красноярск, 2022. С. 34—38.

18. Шерманов И. С. Фальсификация доказательств и результатов оперативно-розыскной деятельности // Научные высказывания. 2022. № 2 (10). С. 27—29.

19. Чечетин А. Е., Шатохин И. Д., Шмидт А. А. Оперативно-розыскная деятельность в решениях Конституционного Суда Российской Федерации: научно-практическое пособие. Барнаул, 2022. 136 с.

20. Елисов П. П. Использование оперативной дезинформации и инсценировки при проведении оперативно-розыскных мероприятий по выявлению и документированию коррупционных преступлений: мнение аналитика // Научный портал МВД России. 2015. № 2 (30). С. 54—60.

21. Елисов П. П. Использование оперативной дезинформации и инсценировки при выявлении и документировании коррупционных преступлений: сборник материалов комплекса международных научно-практических конференций. Санкт-Петербург; Пушкин, 2022. С. 28—38.

22. Образцов В. А., Андреев С. В., Бертовский Л. В. Использование дезинформации при выявлении и расследовании преступлений // Российский следователь. 2005. № 8. С. 2—6.

References

1. A person with a different face: What is a deepfake and why is it dangerous? URL: https://www.5-tv.ru/tabloid/306975/dipfejki-cto-eto-kak-rabotaet-icem-opasno/ (accessed 25.12.2022). (In Russ.)

2. The criminal life of deepfakes. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov (accessed 25.12.2022). (In Russ.)

3. Greshnova N. A., Sitnik V. N. Ensuring public interest in the context of digitalization: problems of criminal law in Russia (on the example of deepfake technology). *Bulletin of the Saratov State Law Academy*, 2022, no. 5 (148), pp. 182—189. (In Russ.)

4. Danilova V. A., Levkin D. M. Legal aspects of regulation of “Deepfake” technology in Russia. *Law and state: theory and practice*, 2022, no. 7 (211), pp. 88—91. (In Russ.)

5. Perina A. S. To the question of the qualification of deepfakes: collection of materials of the international student and scientific conference. Krasnoyarsk: SIBUI of the Ministry of Internal Affairs of Russia Publ., 2022. Issue 24. Pp. 331—333. (In Russ.)

6. Dent S. California cracks down on political and pornographic deepfakes. URL: https://www.engadget.com/2019-10-07-california-deepfake-pornography-politics.html (accessed 22.12.2022). (In Russ.)

7. Ivanov V. G., Ignatovsky Ya. R. Deepfakes: prospects for application in politics and threats to the individual and national security. *Bulletin of the Peoples’ Friendship University of Russia. Series: State and municipal management*, 2020, no. 4, pp. 379—386. (In Russ.)

8. China introduced criminal penalties for publishing deepfakes without explanation. URL: https://rtvi.com/news/v-kitae-vveli-ugolovnoe-nakazanie-za-publikatsiyu-dipfeykov-bez-poyasneniy/ (accessed 25.12. 2022). (In Russ.)

9. Mikheev E. A., Nestik T. A. Disinformation in social networks: state and prospects of psychological research. *Social psychology and society*, 2018, vol. 9, no. 2, pp. 5—20. (In Russ.)

10. Dubonosov E. S. Disinformation of the criminal environment in the implementation of operational-investigative activities. *News of the Tula State University. Economic and legal sciences*, 2021, no. 2, pp. 27—33. (In Russ.)

11. Berdnikov V. L. The subjective side of the crime under article 303 of the Criminal Code of the Russian Federation. *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia*, 2022, no. 1 (100), pp. 87—97. (In Russ.)

12. Burmistrova A. A. Lawful operational-search measure “Trap” in the law enforcement practice of the United States of America and the criteria for its delimitation from the provocation of a crime. *Siberian Anthropological Journal*, 2022, vol. 6, no. 3, pp. 105—110. (In Russ.)

13. Kokurin G. A. On some methods of falsifying the results of operational-search activities. *Russian law: education, practice, science*, 2022, no. 1, pp. 75—80. (In Russ.)

14. Safonov A. Yu. Methods of committing crimes in criminal cases on the falsification of evidence and (or) the results of the ORD. *Altai Legal Bulletin*, 2017, no. 4, pp. 122—127. (In Russ.)

15. Sementsov V. A. Provocation of a crime in the operational-search activity. *Union of criminologists and criminologists*, 2020, no. 4, pp. 45—53. (In Russ.)

16. Sushchenko S. A. The problem of the admissibility of evidence obtained on the basis of operational-search activities as a result of provocation in Russia and foreign countries: some comparative legal aspects. Lukyanov, 2022. No. 3 (92). Pp. 228—234. (In Russ.)

17. Shashin D. G. Operative-investigative measures and provocation: the legality of sanctions and active actions: materials of the All-Russian Scientific and Practical Seminar. Krasnoyarsk, 2022, pp. 34—38. (In Russ.)

18. Shermanov I. S. Falsification of evidence and results of operational-search activities. *Scientific statements,* 2022, no. 2 (10), pp. 27—29. (In Russ.)

19. Chechetin A. E., Shatokhin I. D., Shmidt A. A. Operational-search activity in the decisions of the Constitutional Court of the Russian Federation: scientific and practical guide. Barnaul, 2022. 136 p. (In Russ.)

20. Elisov P. P. The use of operational disinformation and staging during operational-search activities to identify and document corruption crimes: an analyst's opinion. *Scientific portal of the Ministry of Internal Affairs of Russia,* 2015, no. 2 (30), pp. 54—60. (In Russ.)

21. Elisov P. P. The use of operational disinformation and staging in identifying and documenting corruption crimes: a collection of materials from a complex of international scientific and practical conferences. St. Petersburg, Pushkin, 2022, pp. 28—38. (In Russ.)

22. Obraztsov V. A., Andreev S. V., Bertovsky L. V. The use of misinformation in the detection and investigation of crimes. *Russian investigator*, 2005, no. 8, pp. 2—6. (In Russ.)

Информация об авторе

В. Б. Батоев — кандидат юридических наук, доцент.

Information about the author

V. B. Batoev — Candidate of Sciences (Law), Associate Professor.

Статья поступила в редакцию 18.01.2023; одобрена после рецензирования 25.02.2023; принята к публикации 05.03.2023.

The article was submitted 18.01.2023; approved after reviewing 25.02.2023; accepted for publication 05.03.2023.