

Научная статья  
УДК: 343.985.7

## ИСПОЛЬЗОВАНИЕ ДАННЫХ ГЕОПРОСТРАНСТВЕННОЙ РАЗВЕДКИ (GEOINT) ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

**Александр Сергеевич Самоделкин<sup>1</sup>, Сергей Владимирович Тимофеев<sup>2</sup>**

<sup>1</sup>Московский университет МВД России им. В. Я. Кикотя, г. Москва, Российская Федерация, putin@list.ru

<sup>2</sup>Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, tsv.1981@mail.ru

**Аннотация.** В статье рассматривается комплекс теоретических и практических вопросов, связанных с использованием данных геопространственной разведки в оперативно-розыскной деятельности. Авторы проанализировали теоретические обоснования, правовые и организационные основы интеграции геоданных в практику деятельности оперативных подразделений органов внутренних дел, определили ключевые источники такой информации и их дидактический потенциал. Особое внимание уделяется практическим аспектам: методам работы подразделений по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России с геопространственными данными на различных стадиях оперативной работы – от планирования, выявления признаков преступной деятельности до обеспечения оперативно-розыскных мероприятий и процессуального оформления полученных результатов. На основе анализа современных вызовов формулируются проблемные вопросы, требующие разрешения.

**Ключевые слова:** геопространственная разведка, оперативно-розыскная деятельность, информационно-телекоммуникационные технологии, дистанционное зондирование земли, геоинформационные системы, оперативная обстановка, теория ОРД, геопространственная разведка (GEOINT)

**Для цитирования:** Самоделкин, А. С., Тимофеев, С. В. Использование данных геопространственной разведки (GEOINT) при осуществлении оперативно-розыскной деятельности: вопросы теории и практики // Криминалистика: вчера, сегодня, завтра. 2025. Т. 36. № 4. С. 174–185.

## USING GEOSPATIAL INTELLIGENCE DATA IN OPERATIONAL SEARCH ACTIVITIES: THEORY AND PRACTICE

**Alexander S. Samodelkin<sup>1</sup>, Sergey V. Timofeev<sup>2</sup>**

<sup>1</sup>V. Ya. Kikot Moscow University of the MIA of the Russia, Moscow, Russian Federation, putin@list.ru

<sup>2</sup>East Siberian Institute of the MIA of the Russian Federation, Irkutsk, Russian Federation, tsv.1981@mail.ru

**Abstract.** This article examines a range of theoretical and practical issues related to the use of geospatial intelligence data in investigative operations. The authors analyze the theoretical underpinnings, legal framework, and organizational foundations for integrating geospatial data into the operational practices of law enforcement agencies, identifying key sources of such information and their educational potential. Particular attention is paid to practical aspects: the methods used by units to combat the illegal use of information and communication technologies (ICTs) of the Ministry of Internal Affairs of Russia (hereinafter, ICTs) with geospatial data at various stages of operational work—from planning and identifying signs of criminal activity to supporting investigative operations and formalizing the results. Based on an analysis of current challenges, problematic issues requiring resolution are identified.

**Keywords:** geospatial intelligence, operational-investigative activities, information and telecommunications technologies, remote sensing of the earth, geoinformation systems, operational situation, operational-investigative activity theory, geospatial intelligence (GEOINT)

**For citation:** Samodelkin, A. S., Timofeev, S. V. Ispol'zovanie dannykh geospatial'noy razvedki (GEOINT) pri osushchestvennyi operativno-rozysknoy deyatel'nosti: voprosy teorii i praktiki [Using geospatial intelligence data in operational search activities: theory and practice]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025. vol. 36 no. 4. pp. 174–185 (in Russ.)

### **Введение**

Раскрытие преступлений является одной из важных задач оперативно-розыскной деятельности (далее – ОРД). Для решения этой задачи органы, осуществляющие ОРД, руководствуясь принципами конспирации, сочетания гласных и негласных методов и средств, используют современные достижения науки, техники и цифровых технологий, которые в значительной степени повышают эффективность проведения оперативно-розыскных мероприятий (далее – ОРМ).

К числу таких технологий относятся системы распознавания лиц и анализа больших данных (BigData), позволяющие выявлять преступные схемы и устанавливать связи между фигурантами. Использование криптоанализа и специального программного обеспечения помогает расшифровывать электронную переписку

преступников, действующих в DARKNET.

Кроме того, геоинформационные системы и технологии сотового позиционирования позволяют с высокой точностью определять местонахождение разыскиваемых лиц и моделировать их возможные маршруты.

Важнейшую роль играет компьютерная криминалистика, которая обеспечивает изъятие, сохранение и анализ цифровых доказательств с электронных носителей. Это направление стало неотъемлемой частью расследования практически любого преступления, поскольку преступная деятельность все чаще перемещается в киберпространство.

### **Основная часть**

Использование сил, методов и средств ОРД, в сочетании с современными возможностями компьютерной криминалистики, обеспечивают повышение эффективности решения задач ОРД и повышают качество опе-

ративного сопровождения расследования уголовных дел.

Исследованием вопросов повышения эффективности раскрытия преступлений в ходе осуществления ОРД и криминалистического обеспечения их расследования занимались такие видные ученые теории оперативно-розыскной деятельности и ученые-криминалисты, как В. Г. Бобров, В. М. Аتماжитов, Н. С. Железняк, В. Ф. Луговик, А. Л. Осипенко, О. П. Грибунов, В. Ф. Васюков и др.

Заслуженный юрист Российской Федерации, профессор Н. С. Железняк отмечал, что «перечень оперативно-розыскных мероприятий, как стрессовой элемент оперативно-розыскной деятельности, и их наименования не отвечают потребностям теории и практики профессионального сыска» [1, с.80].

Ранее схожее мнение высказывали профессора В. Г. Бобров и В. М. Аتماжитов, подчеркивающие, что оперативно-розыскные мероприятия «далеко не исчерпывают всего содержания оперативно-розыскной деятельности. Наряду с ними органы дознания (указанные в п. 1 ч. 1 ст. 40 УПК РФ) для решения задач по борьбе с преступностью используют также оперативно-розыскные методы, проводят другие действия» [2, с. 24].

Такие видные ученые, как В. Ф. Луговик и А. Л. Осипенко отмечали, что необходимость совершенствования правового регулирования ОРД в современных условиях «определяется и связанными с развитием информационных технологий сложными социальными и технологическими процессами, вызывающими существенное изменение закономерностей образования и концентрации оперативно значимой информации. Постоянно расширяется спектр технических источников оперативно-розыскных данных, к которым могут быть отнесены различные информа-

ционные системы государственных органов и коммерческих структур, в том числе операторов связи, потоки данных от разнообразных датчиков (радиочастотных идентификаторов, GPS-трекеров и т. п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации, сообщения из социальных сетей и иных мест сетевого общения объектов оперативного интереса» [3, с. 8].

Нельзя обойти стороной и мнение выдающихся ученых-криминалистов А. В. Варданяна и О. П. Грибунова, которые справедливо отмечают, что расследование преступлений – это «сложный и трудоемкий процесс и для достижения положительных результатов данной деятельности требуются определенные знания и умения» [4, с. 23].

В этом контексте В. Ф. Васюков, С. В. Расторопов и Д. Ф. Флоря совершенно справедливо отмечают, что процесс информатизации «кардинально изменил способы взаимодействия между людьми, государством и бизнесом. Сегодня цифровые технологии позволяют мгновенно обмениваться данными, автоматизировать сложные процессы и принимать решения на основе анализа больших объемов информации...» [5, с. 5].

Солидаризируясь с мнением ведущих ученых, полагаем, что дальнейшее развитие теории ОРД и разработки криминалистических методик расследования отдельных видов преступлений, при которых использовались информационно-телекоммуникационные технологии (далее – ИТТ), нельзя представить без дальнейших исследований современных технологий поиска, сбора и анализа информации, представляющей оперативный интерес. К числу таких технологий в настоящее время относятся данные геопро пространственной разведки (GEOINT – сокращение от

Geospatial Intelligence, от англ. «Геопространственная разведка»).

Геопространственная разведка (далее – GEOINT) представляет собой процесс сбора, анализа и применения геопространственных данных для получения разведывательной информации, в том числе комплекс методов получения и анализа данных о местоположении объектов, открывающий новые возможности для расследования преступлений<sup>1</sup>.

GEOINT включает в себя как данные о местоположении (географические координаты), так и информацию о физических характеристиках объектов на Земле.

В настоящее время существуют различные виды технологий, которые используются в геопространственной разведке:

1. Спутниковая съёмка. Один из главных источников геоданных, предоставляющая детальные изображения местности в реальном времени.

2. Географические информационные системы (далее – ГИС). ГИС представлена в виде программного обеспечения, предназначенного для обработки и анализа геопространственной информации.

3. Беспилотные летательные аппараты (далее – БПЛА). БПЛА используются для оперативного сбора геоданных в сложных условиях.

4. Георадарные исследования, позволяющие анализировать структуру поверхности и подземных объектов.

5. Мобильные данные способствуют отслеживанию перемещения людей и транспортных средств.

<sup>1</sup> GEOINT — Geospatial intelligence или геолокационная разведка // URL : <https://dataqa.ru/geoint-geospatial-intelligence-ili-geolokatsionnaya-razvedka/> [Электронный ресурс] дата обращения 20.08.2025.

Согласно российскому уголовно-процессуальному законодательству, установление места, времени и обстоятельств совершения преступления является центральным элементом доказывания (ст. 73 УПК РФ). В этом контексте пространственно-временная информация играет ключевую роль в формировании доказательственной базы по уголовным делам.

Современные навигационные системы предоставляют широкие возможности для получения информации о местонахождении объектов оперативной заинтересованности и фигурантов расследования уголовных дел.

Основными источниками геоданных являются:

- мобильные устройства с функцией определения местоположения;
- картографические приложения со встроенной функцией отслеживания маршрута;
- системы сотовой связи с возможностью определения координат абонента;
- специализированное оборудование для криминалистического исследования контента мобильных устройств;
- тактические возможности использования геопространственной информации.

Анализ геопространственных данных позволяет решать такие задачи, как:

- установление фигурантов и свидетелей преступления;
- розыск лиц и установление местонахождения похищенного имущества;
- проверка алиби подозреваемых;
- установление маршрута движения и времени нахождения преступника в определенном месте;
- проверку показаний о месте и времени события.

Процессуальное закрепление геопространственных данных осуществляется посредством составления протоколов следственных действий (обыска, выемки, осмотра места происшествия), заключений компьютерно-технических экспертиз и допросов специалистов.

Ряд ученых, таких как Е. И. Третьякова, А. А. Шаевич, В. А. Родивилина справедливо отметили, что разное целевое назначение специальных познаний в уголовном судопроизводстве и оперативно-розыскной деятельности «обуславливает неодинаковую правовую регламентацию их применения в следственно-судебной и оперативно-розыскной практике» [6, с. 38].

В этом контексте С. В. Тимофеев совершенно справедливо отмечает, что вектор российского государства, направленный на адаптацию отечественного законодательства к современным вызовам и угрозам цифровой преступности «приносит положительные результаты, но не в полной мере использует имеющиеся резервы в организации использования всего потенциала институтов гражданского общества» [7, с. 224].

Как и в любой сфере человеческой деятельности, при применении геопространственной разведки возникает комплекс проблем, связанных с необходимостью обеспечения сохранности электронных данных, сложностью интерпретации полученных сведений, потребности в квалифицированных специалистах и потребности совершенствования правового регулирования данной сферы.

Дальнейшее развитие использования геопространственной информации в уголовном процессе связано с совершенствованием технических средств получения данных, разработкой новых методик криминалистического исследования и усовершенствованием процессуальных меха-

низмов закрепления доказательств. Поэтому использование результатов геопространственной разведки в уголовном процессе является перспективным направлением развития криминалистической техники.

С учетом того, что GEOINT представляет собой комплексный анализ изображений и данных, отражающих физические характеристики и активность на земной поверхности, в сферу его применения входит изучение как антропогенных объектов, так и природных компонентов, включая рельеф местности, растительный покров и метеорологические условия.

Зарождение концепции геопространственной разведки тесно связано с военной сферой. Первые шаги в этом направлении были сделаны во время мировых войн, когда военные начали активно применять аэрофотосъемку для мониторинга дислокации и передвижения вражеских сил. Командование быстро оценило стратегическую значимость воздушной разведки, которая давала существенное преимущество в планировании боевых операций.

Развитие GEOINT прошло значительный путь от примитивной аэрофотосъемки до современной высокотехнологичной дисциплины.

Качественный скачок в ее развитии произошел с началом космической эры и появлением спутниковых технологий, которые открыли новые возможности для сбора и анализа геопространственной информации.

Сегодня GEOINT представляет собой многогранную область, объединяющую различные методы сбора и обработки данных о земной поверхности, что позволяет использовать её не только в военных, но и в гражданских целях, включая экологический мониторинг, городское планирование и управление чрезвычайными ситуациями.



Эпоха холодной войны стала переломным этапом в эволюции космической геопрограмственной разведки. Противостояние между США и СССР стимулировало активное развитие технологий спутниковой разведки, поскольку обе державы осознали критическую важность космического наблюдения для национальной безопасности.

Революционным событием стал запуск спутника Corona в 1960 году, ставшего первым успешным разведывательным космическим аппаратом США. Инновационная технология того времени предусматривала использование пленочных камер для получения детальных снимков земной поверхности. Полученные материалы доставлялись на Землю в специальных капсулах, которые перехватывались в воздухе специальными самолетами.

В последующие десятилетия, на протяжении 1960-х и 1970-х годов, технологическая гонка между сверхдержавами привела к появлению все более совершенных разведывательных спутников.

Особую роль сыграли американские аппараты серии Keyhole, находившиеся под управлением Национального разведывательного управления (NRO) [8, с. 30]. Эти спутники обеспечивали США критически важной информацией, включая точное местоположение советских ракетных баз и других стратегически важных объектов, что имело решающее значение в контексте глобального противостояния.

Таким образом, период холодной войны не только стимулировал развитие космических технологий, но и заложил фундамент современной системы геопрограмственной разведки, многие принципы которой актуальны и сегодня.

Если на начальном этапе развития геопрограмственной разведки

спутники использовались исключительно в интересах государственных структур для военных и разведывательных задач, то в 1990-е годы ситуация кардинально изменилась.

На рынок вышли частные компании, предлагающие услуги спутниковой съемки. Такие аппараты, как IKONOS и QuickBird, открыли доступ к высококачественным спутниковым изображениям не только для государственных организаций, но и для коммерческих структур, что стало революционным прорывом в области распространения геопрограмственной информации.

В последующие годы, на протяжении 2000-х, коммерческий сектор геопрограмственной разведки продемонстрировал устойчивый рост и совершенствование технологий.

Лидеры отрасли, включая такие компании, как DigitalGlobe (ныне часть Maxar Technologies) и Airbus Defence and Space, развернули целые группировки спутников, способных обеспечивать съемку с разрешением менее одного метра.

Современные коммерческие операторы играют ключевую роль в решении широкого спектра задач: от оперативного реагирования на чрезвычайные ситуации и экологического мониторинга до множества других прикладных направлений, что существенно расширило сферу применения геопрограмственной разведки в гражданском секторе.

В XXI веке технологии геопрограмственной разведки совершили качественный скачок в развитии.

Современные спутники GEOINT превратились в многофункциональные платформы, оснащенные передовыми датчиками, значительно превосходящими возможности классической оптической съемки. На борту космических аппаратов устанавливаются комплексные системы, включающие радиолокационные

станции с синтезированной апертурой (SAR), гиперспектральные камеры и инфракрасные датчики, что позволяет получать максимально полную картину земной поверхности и происходящих на ней процессов.

Революционным прорывом стало внедрение технологий оперативной обработки данных. Благодаря развитию высокоскоростных каналов связи и бортовых систем обработки информации, современные спутники способны передавать разведывательные данные в режиме, максимально приближенном к реальному времени. Это существенно ускорило процесс получения критически важной информации для лиц, принимающих решения, что особенно ценно при проведении военных операций и ликвидации последствий стихийных бедствий.

Значительным шагом вперед стало развитие концепции спутниковых группировок малого класса. Компании вроде Planet Labs и Capella Space создали масштабные созвездия из небольших спутников, масса которых зачастую не превышает 100 килограммов<sup>2</sup>. Ключевое преимущество таких группировок заключается в высокой частоте наблюдения за интересующими территориями. Более того, снижение стоимости запуска и эксплуатации малых спутников сделало технологии геопрограмственной разведки доступнее для широкого круга организаций, что способствовало демократизации использования GEOINT-данных в различных сферах деятельности.

Один из распространенных

<sup>2</sup> «Всевидающее око» компании Capella Space: предвестник революции в спутниковой разведке // Электронный ресурс. URL : <https://topwar.ru/178436-vsevidjaschee-oko-kompanii-capella-space-predvestnik-revoljucii-v-sputnikovoj-azvedke.html?ysclid=mi5jz3fc7o434284124>  
Дата обращения: 20.09.2025.

подходов при проведении геопрограмственной разведки заключается в выделении значимых объектов и признаков на изображении, при этом структура поиска по данным источникам информации идет от глобальных источников к локальным.

Принцип «от большего к меньшему» подразумевает определение страны, города или региона, основываясь на глобальных признаках. На основании полученных с помощью глобальных источников «подсказок» по локальным признакам определяется точное местоположение.

Некоторые характерные особенности изображения могут быть как локальными, так и глобальными, например, дорожный знак автомагистрали, который с одной стороны, может указать на страну или город, в котором сделана фотография, с другой стороны — может использовать данный указатель как ориентир при поиске точного местоположения в определенной стране. Это может быть дорожная развязка, и указатель несет информацию о съездах или расстоянии до ближайших населенных пунктов, за счет чего упрощается поиск точного местоположения.

Геопрограмственная разведка опирается на изображения и видеозаписи, анализ их содержимого, а также геопрограмственную информацию.

Оперативные подразделения по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (далее – УБК) наиболее часто и эффективно используют в своей аналитической деятельности метод геопрограмственной разведки, заключающийся в анализе

содержимого изображения, видеозаписи и их контекста для понимания, где и кем они были сделаны.

Разведывательно-аналитический цикл GEONTзаканчивается на стадии использования поисковика изображений, который находит оригинал, где может быть указано, где и как сделана фотография или видеозапись. К таким общедоступным и эффективным веб-ресурсам относятся:

– сервис «Google Earth» (адрес: <https://eah.google.com/web/>), позволяющий искать на карте города достопримечательности, парки и т. д. Именно там содержится наибольшее количество панорам улиц и находятся ответы на разведывательную задачу;

– сервис «DupliChecker» (адрес: URL : <https://www.duplichecker.com/?ref=aitoolnet.com>) способен выполнять обратный поиск фотоизображений. Для этого следует загрузить изображение или ввести ключевое слово, связанное с изображением, которое необходимо изучить. Учитывая, что в сети доступны большие объемы фотографий, представляется сложным отсортировать их все, чтобы найти искомые, их источники (совпадение фотографий) и сопутствующую информацию.

Непосредственно перед тем, как поисковые системы изображений вернут совпадающие результаты, они быстро проверят загруженное изображение с рядом других изображений в своих базах данных, чтобы гарантировать наиболее точные результаты. Обычно, если они доступны, поисковые системы могут использовать метаданные изображения, такие как имя файла изображения, дата, используемая камера и т. д.

При наличии фотоизображения участка местности можно использовать поисковые сервисы «Яндекс» и «Google» («Картинки», «Карты»).

Особое внимание необходимо уделять конкретным объектам (различные вывески, транспортные средства, уникальные объекты и т. п.) с последующим проведением их перекрестной сверки путем просмотра сервисов «Картинки» и «Карты», в том числе в режиме «Панорама» с целью привязки участка местности к конкретному адресу.

Решить эту задачу может веб-сервис «ТопоExport» (адрес: <https://topoexpo.com/>), являющийся эффективным инструментом для изучения топографических особенностей местности. Достаточно выделить нужный сектор на карте и нажать кнопку «Preview», после чего утилита сгенерирует превью топографии и архив с более детальным отчетом.

Существует еще множество инструментов и специализированных программ, позволяющих определить не только место, но и время, в которое был сделан снимок:

– онлайн-сервисы «Shadowmap» и «ShadeMap» («Моделирование теней») помогают по определенной местности на карте рисовать тень и за счет этого определять время фотосъемки;

– онлайн-сервис «Suncalc» по заданной дате показывает расположение солнца в любой промежуток времени. Если в кадре нет солнца, то измерив на фотографии высоту объекта и длину отбрасываемой тени, можно определить время создания снимка;

– онлайн-ресурс «Geonames» содержит географическую базу данных об именах локаций по всем странам мира и насчитывает около



11 миллионов записей. Поддерживает названия на разных языках стран мира.

Допустим, на изображении зафиксировано здание или магазин с названием на арабском языке. В этой ситуации невозможно понять, что обозначает данная надпись, но указанный веб-ресурс позволяет вырезать из изображения часть, содержащую название магазина, и воспользоваться функцией перевода «Яндекс. Переводчик».

После чего результат вставить в поиск сайта «Geonames». Если данное название содержится в базе данных сайта, то он отобразит на карте все полученные результаты.

Веб-ресурсы с помощью которых также возможно определить местоположение по изображению:

- «Satalites Pro» – спутниковая информация;
- «Wikimapia» – данные о постройках;
- «Zoom Earth» – температуры, пожары, осадки;
- «Peak Visor» содержит данные о более чем миллионе горных вершин по всему миру. Рисует их контуры, часто используется для опознавания локации по очертанию рельефа на заднем плане.

Пример поиска местоположения по фотографии. Для практики GEOINT создано множество интернет-ресурсов и форумов. Для начинающих и продвинутых пользователей наиболее подходящим является «Geoguessr».

С развитием искусственного интеллекта и специального программного обеспечения все чаще в преступных схемах появляются фото- и видеоматериалы, созданные с целью распространения недостоверной или искаженной информации – «Дипфейк».

«Дипфейк» («DeepFake») представляет собой методику компьютерного синтеза

изображения, основанную на искусственном интеллекте, которая используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики.

Ключевым компонентом для создания подделки с помощью технологии «дипфейк» является машинное обучение. «Дипфейки» полагаются на компьютерные системы искусственного интеллекта, называемые искусственными нейронными сетями, которые предназначены для распознавания закономерностей среди большого массива данных.

Существует общий принцип создания «дипфейков» – GAN, представляющую собой генеративно-сопоставительную сеть (Generative adversarial network). Это алгоритм машинного обучения, построенный на соревновании двух нейросетей. Одна зовется «Генератор», она создает фальшивки, другая – «Дискриминатор» – выступает в роли эксперта, который пытается отличить подделку от оригинала. Чем лучше «Генератор» обманывает «Дискриминатора», тем правдоподобнее выглядит «дипфейк».

Сеть GAN – это самоучитель для нейросетей, способная копировать в том числе и голос. Чтобы максимально достоверно воспроизводить человеческую речь нейросети достаточно всего несколько минут аудиозаписи для обучения.

Преступники активно используют «дипфейки» для кражи персональных данных и кражи онлайн-личности, распространения дезинформации в обществе, финансового шантажа, мошенничества и автоматизированных кибератак.

В первую очередь для самостоятельного анализа видеоизображения на наличие

монтажа следует обратить внимание на такие базовые факторы:

- излишняя пикселизация, дефекты, нечеткое и смазанное изображение, дублирование элементов;

- неестественная мимика, особенно при моргании, движении бровей и губ;

- низкое качество видео, за которым нередко пытаются скрыть некорректную работу нейросетей;

- отличия в телосложении, причёске и голосе от оригинала. Злоумышленники нередко подбирают похожих по типу актеров, а голос может быть также скорректирован с помощью специальной технологии, например, в программах «RealTimeVoiceCLoning», «Resemble» и «Descript»;

- в наиболее популярных решениях заменяется только лицо, поэтому можно заметить границу наложения лица, различие в тенях, освещенности и оттенке кожи.

Технологии эволюционируют быстро, и «дипфейки» последнего поколения выполнены очень качественно. Зачастую очень сложно отличить подделку невооруженным глазом. В этих случаях необходимо использовать специальные программы распознавания, которые анализируют видеоизображения и замечают незначительные искажения, возникающие в процессе создания «дипфейка».

Это позволяют программы, с помощью которых можно обнаружить «дипфейки»:

1. «Forensically» – простой и понятный набор бесплатных инструментов для анализа изображений.

2. «Image Edited» – бесплатный сервис, который ищет изменения в фотографиях, анализирует изображение на уровне пикселей и их цветов.

3. «Ghiro» – автоматически анализирует огромное количество

изображений с целью проведения криминалистического анализа.

4. «Truepic» – проверяет фото и видео на предмет внесенных изменений.

5. «KaiCatch» – распознает аномалии и искажения в фото и видео с помощью искусственного интеллекта.

6. «Microsoft Video Authenticator» оценивает фото и видео и определяет вероятность монтажа.

7. «Deerware» – бесплатный инструмент для анализа видео.

### **Выводы и заключение**

В качестве решения этих Перспективы развития геопромышленной разведки открывают широкие возможности для инноваций в сфере спутниковых технологий.

Важным вектором развития становится многодоменная интеграция систем. В условиях стирания границ между воздушными, космическими и киберпространственными операциями спутники GEOINT должны обеспечивать бесперебойную работу во всех этих сферах. Это потребует создания принципиально новых технологических решений и архитектур, способных эффективно объединять и обрабатывать информацию из различных источников, что предопределяет их интеграцию в практику деятельности оперативных подразделений ОВД.

Дополнительным драйвером развития становится растущая потребность в непрерывном мониторинге территорий. Современные вызовы требуют возможности постоянного наблюдения за интересующими объектами и территориями, что ставит перед разработчиками спутников GEOINT задачу создания более совершенных систем длительного наблюдения с высокой точностью и надежностью.

Таким образом, интеграция цифровых технологий в ОРД и уголовно-процессуальную деятельность трансформировала традиционные

подходы к раскрытию преступлений, сделав оперативно-розыскной процесс более прогнозируемым, точным и результативным. Однако это же порождает и новые вызовы, связанные с необходимостью правового регули-

рования использования таких технологий и обеспечения защиты прав граждан.

#### СПИСОК ИСТОЧНИКОВ

1. Железняк, Н. С. Вопросы актуализации Федерального закона "Об оперативно-розыскной деятельности". – 2-е издание, переработанное и дополненное. – Красноярск : Красноярский государственный аграрный университет, 2022. 236 с.
2. Аتماжитов, В. М., Бобров, В. Г. Оперативно-розыскные мероприятия: актуальные вопросы теории и практики // Государство и право. 2005. №. 3. С. 23–31.
3. Луговик, В. Ф., Осипенко, А. Л. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. 2015. №. 4. С. 7–12.
4. Варданян, А. В., Грибунов, О. П. Современная доктрина методико-криминалистического обеспечения расследования отдельных видов преступлений // Вестник Восточно-Сибирского института МВД России. 2017. №. 2 (81). С. 23–35.
5. Васюков, В. Ф., Расторопов, С. В., Флоря, Д. Ф. Получение и использование абонентской информации при расследовании преступлений. – Орел : Картуш, 2025. 324 с.
6. Третьякова, Е. И., Шаевич, А.А., Родивилина, В.А. Раскрытие и расследование преступлений по горячим следам: учебное пособие. – Иркутск: Восточно-Сибирский институт МВД России, 2022. 48 с.
7. Тимофеев, С. В., Пороховой, Э. Ю. Выявление и предупреждение преступлений в сети интернет: проблемы и пути их решения // Вестник Восточно-Сибирского института МВД России. 2021. № 4(99). С. 220–229.
8. Павлов, Н. В. Разведка на основе средств космического базирования // Авиационные системы. 2013. № 5. С. 28-41.

#### REFERENCES

1. ZHeleznyak, N. S. Voprosy aktualizacii Federal'nogo zakona "Ob operativno-rozysknoj deyatel'nosti" [Issues of actualization of the Federal Law "On Operational-Search Activities"]. Krasnoyarsk, 2022, 236 p. (in Russian).
2. Atmazhitov V. M., Bobrov V. G. Operativno-rozysknye meropriyatiya: aktual'nye voprosy teorii i praktiki [Operational-search measures: actual issues of theory and practice.]. Gosudarstvo i pravo. – State and Law. 2005, no. 3, pp. 23-31. (in Russian).
3. Lugovik, V. F., Osipenko, A. L. Operativno-rozysknaya deyatel'nost' organov vnutrennih del: perspektivy sovershenstvovaniya pravovogo regulirovaniya [[Operational-search activities of internal affairs bodies: prospects for improving legal regulation]]. Vestnik Voronezhskogo instituta MVD Rossii – Vestnik of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2015, no. 4, pp. 7-12. (in Russian).
4. Vardanyan, A. V., Gribunov, O. P. Sovremennaya doktrina metodiko-kriminalisticheskogo obespecheniya rassledovaniya otdel'nyh vidov prestuplenij [Modern doctrine of methodo-forensic support for the investigation of certain types of

crimes]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii. – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2017, no. 2 (81), pp. 23–35. (in Russian).

5. *Vasyukov, V. F.* Poluchenie i ispol'zovanie abonentskoj informacii pri rassledovanii prestuplenij [Obtaining and Using Subscriber Information in the Investigation of Crimes]. Orel : Kartush, 2025, 324 p. (in Russian).

6. *Tret'yakova, E. I.* Raskrytie i rassledovanie prestuplenij po goryachim sledam [Disclosure and investigation of crimes in hot pursuits]. Irkutsk, 2022, 48 p. (In Russian). (in Russian).

7. *Timofeev, S. V., Porohovoj, E. YU.* Vyyavlenie i preduprezhdenie prestuplenij v seti internet: problemy i puti ih resheniya [Identification and prevention of crimes on the Internet: problems and ways to solve them]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2021, no. 4(99), pp. 220–229. (in Russian).

8. *Pavlov, N. V.* Razvedka na osnove sredstv kosmicheskogo bazirovaniya [Space-Based Intelligence]. Aviacionnye sistemy – Aviation Systems. 2013, no. 5, pp. 28-41. (in Russian).

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

**Самоделкин Александр Сергеевич**, доктор юридических наук, доцент, профессор кафедры оперативно-разыскной деятельности и специальной техники. Московский университет МВД России имени В. Я. Кикотя. 117997, Российская Федерация, г. Москва, ул. Академика Волгина, д. 12

**Тимофеев Сергей Владимирович**, кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности и специальной техники в органах внутренних дел. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, Иркутск, ул. Лермонтова, 110.

#### INFORMATION ABOUT THE AUTHORS

**Alexander S. Samodelkin**, Doctor of Law, Associate Professor, Professor of the Department of Operational-Investigative Activities and Specialized Equipment. Kikot Moscow University of the MIA of Russia. 12, Academician Volgina st., Moscow, Russian Federation, 117997.

**Sergey V. Timofeev**, Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of Operational Investigative Activities and Special Equipment in Internal Affairs Bodies. East Siberian Institute of the MIA of Russia. 110, st. Lermontova, Irkutsk, Russian Federation, 664071.