Физика волновых процессов и радиотехнические системы
*2023. Т. 26, № 3. С. 116–122*

DOI 10.18469/1810-3189.2023.26.3.116-122
УДК 343.9
Оригинальное исследование

*Дата поступления* 13 декабря 2022
*Дата принятия* 17 января 2023
*Дата публикации* 27 сентября 2023

# Анализ возможностей искусственного интеллекта для расследования мошенничества

*Д.С. Клюев*[1], *А.Б. Смушкин*[2], *Ю.В. Соколова*[1], *С.Е. Платонов*[2]

[1] Поволжский государственный университет телекоммуникаций и информатики
443010, Россия, г. Самара,
ул. Л. Толстого, 23
[2] Поволжский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России)
410003, Россия, г. Саратов,
ул. им. Радищева А.Н., 55

*Аннотация* – **Обоснование.** В результате цифровизации общества растет число мошеннических действий с применением информационно-телекоммуникационных технологий. Технологическая сложность расследования такова, что требует применения аналогичных инструментов в следственных и оперативно-розыскных мероприятиях. Таким инструментом может являться искусственный интеллект. **Цель.** Определить потенциал искусственного интеллекта в следственных и оперативных действиях. **Методы.** Методом анализа проведена оценка существующих решений для применения в следственных и оперативных мероприятиях, таких как распознавание лица, основанное на правилах Хаара, программ имитаторов и управления голосом, решений сервиса «Инцидент менеджмент», АДИС «Папилон», ГИС «Зеркало», проект «Форвер», ИС «Образ++», возможностей машинного обучения, нейронных сетей. **Результаты.** Показаны некоторые актуальные решения, требующие интеграции в единую систему технологических и интеллектуальных решений (искусственный интеллект) для следственных действий и оперативно-розыскных мероприятий. **Заключение.** Приведены современные автоматизированные информационные инструменты, требующие их объединения в единую интеллектуальную технологическую систему (искусственный интеллект) расследования преступлений.

*Ключевые слова* – следственные действия; классическое и цифровое мошенничество; машинное обучение; нейросети; цифровые следы; интеллектуальная идентификация; искусственный интеллект.

Примеров мошеннических действий с применением современных технологий на сегодняшний день множество. Например, предоставление дубликатов фотографий аварий для получения выплат от страховых компаний. Подделка основных персональных данных – «создание» человека по разным идентификаторам: номер СНИЛС, номер и серия паспорта, серия полиса ОМС. Так, в аналитических источниках, указано, что мошенничество с использованием поддельных удостоверений личности является самым быстрорастущим финансовым преступлением в США [1].

По данным RTM Group, в 2021 г. зарегистрировано 517 722 преступлений, связанных с хищениями с использованием информационных технологий, что всего на 1,44 % больше, чем в 2020 г. (510 396 преступлений), но практически вдвое превышает 294 409 зарегистрированных преступлений в 2019 г.

Хищения в сети Интернет характеризуются высокой скрытностью и низкой раскрываемостью, в том числе из-за возможности дистанционного совершения данных преступлений. Раскрываемость категории дел составляет в среднем 20 % ежегодно.

Самыми распространенными преступлениями в данной сфере являются мошенничество (ст. 159 УК РФ, 159.3, 159.6) – в 2021 г. зарегистрировано 249 249 дел, и кража (п. г ч. 3 ст. 158 УК РФ) – 156 792 дела.

По опубликованным данным распространенными сферами мошенничества являются:

- сделки с недвижимостью (фиктивные договоры аренды помещения, ипотеки, купли-продажи);
- заключение гражданско-правовых договоров (купля-продажа товаров в Интернете, к примеру б/у автомобилей на сайте Авито; оказание туристических и строительных услуг);
- социальные сети, сайты знакомств (для продолжения общения лица просили перевести денежные средства, объясняя это тяжелой жизненной ситуацией).

Наиболее распространенными способами совершения хищений при помощи интернет-технологий являются следующие:

- дистанционное подписание фиктивного договора;
- инвестиции в фейковые «биржи», розыгрыши;
- фишинговые атаки.

Ущерб от действий телефонных и интернет-мошенников составил 150 миллиардов рублей в 2021 г. Данные о размерах ущерба в результате

platonovse@mail.ru (*Платонов Сергей Евгеньевич*)

хищений при помощи интернет-технологий разнятся в зависимости от источников, но при этом остаются весьма высокими. По данным МВД, за 2021 г. ущерб от телефонных и интернет-мошенников достиг 45 миллиардов рублей (статистика обусловлена фактическим количеством зарегистрированных преступлений). Данные социологических опросов и исследований выявили ущерб от действий телефонных и интернет-мошенников в размере около 150 миллиардов рублей за 2020 г., и результаты исследований окончательно не подведены [2].

Причиной вариативности данных преступлений будет являться разнообразие социальной активности человека, степени социализации общества, которая требует автоматизации общественных процессов, по причине огромного количества создаваемых данных и запросов к ним.

Очевидно, что уже сегодня классический инструментарий следователей и дознавателей недостаточен, а по факту они находятся в роли догоняющих за подобными преступлениями.

И пути решения должны быть адаптивны и ситуативными. С позиции оперативно-розыскной деятельности и экономической точки зрения расследование будет успешнее не только с увеличением числа следователей, но и с наделением их высокотехнологическими инструментами. Таким инструментом может являться искусственный интеллект с множеством его возможностей, которые рассмотрим в данной работе.

Работа искусственного интеллекта заключается в сочетании большого объема данных с возможностями быстрой, интерактивной обработки этих данных интеллектуальными алгоритмами, что позволяет программам автоматически обучаться на базе закономерностей и признаков, содержащихся в данных [3].

К признакам системы искусственного интеллекта относится рациональность, которая характеризует возможность принятия ею ситуационно и причинно обусловленного, наилучшего из возможных решения при соблюдении неких условно стабильных правил. В рассматриваемом случае использование системы искусственного интеллекта применительно к следственной деятельности следует понимать как комбинацию норм уголовного материального права, уголовно-процессуальных норм, а также технико- и тактико-криминалистических рекомендаций. Автономность – независимость системы от внешних факторов. Она может быть ресурсной (к примеру, энергетической) и информационной. Учитывая, что деятельность следователя направлена на работу с информационными источниками, приоритет имеет именно информационный аспект автономности систем искусственного интеллекта, ориентированных на обработку информации и принятие решений; ресурсная автономность же более характерна для роботизированных систем, которые в целом также могут быть использованы в следственной деятельности. Распознавание – определение относимости входящих объектов (образов) к единичной искомой группе. Примером реализации такой функции (с точки зрения решаемых задач, но не принципов работы) может служить АДИС «Папилон», которая с большими условностями может быть отнесена к системам искусственного интеллекта (экспертного типа, а не на базе машинного обучения). К задачам распознавания относятся идентификации человека по его внешности, номера транспортного средства, группы генов в геноме и пр. В этом случае предполагаемых групп существует две: искомые объекты и все остальные объекты, не соответствующие интересам расследования. Классификация – распределение данных по группам согласно заданным параметрам, к примеру при оценке достоверности информации в Интернете, определении способов подделок и подлогов. Соответственно, на конечной стадии дихотомического деления происходит ответ на вопрос «Относится ли данный объект к искомой группе?». Предсказание – определение будущего состояния определенной информационной системы или отдельных ей показателей, к примеру динамики преступности в регионе, места нахождения преступника или совершения следующего эпизода многоэпизодного преступления и пр. К этой же группе задач относится интеллектуальное формирование юридических документов. В этом случае предъявляется совокупность статистических данных, на основании анализа которых система должна сделать предположение о будущем состоянии и вариантах развития источников данных. Ответ в этом случае тоже является бинарным: будет ли данный объект в будущем (или неизвестном настоящем) иметь заданную характеристику, или нет. Следует также упомянуть, что интеллектуальные системы могут использоваться как элемент навигации по справочным базам данных правового, криминалистического или иного характера. С технической точки зрения системой искусственного интеллекта экспертного типа (а не на основе машинного обучения) может являться

любая система управления базой данных, однако с точки зрения настоящей работы интерес представляют возможности повышения эффективности именно деятельности следователя, а не увеличение его знаний за счет внешнего их источника, что, впрочем, также крайне важно [4].

Искусственный интеллект в правоохранительной деятельности – это технико-технологическая способность решать следственные задачи, используя различные машинные технологии как криминалистические инструменты. В работе будет осуществлена попытка осмысления цифровой архитектуры для расследования классического и цифрового мошенничества.

Основа архитектуры – база данных преступлений одной правоохранительной службы. Создание единой базы правоохранительных органов только повысит ее уязвимость, а территориальная разветвленность будет способствовать ее автономности. На первоначальном этапе в структуре правоохранительной службы должны появиться аналитические отделы, создающие данную базу и вносящие в нее данные прошлых лет. Оперативную информацию вносят действующие следователи и дознаватели. Естественным будет создание внутренней сети и сети дата-центров на территории Российской Федерации.

Следующей ключевой многослойной надстройкой будет являться построение логики будущих решений. По сути, это уже программное решение, которое с помощью технологий машинного обучения будет формировать решение, повышающее эффективность следственных действий. Машинное обучение как процесс становления искусственного интеллекта и его инструменты позволят автоматизировать процесс извлечения известных и построения неизвестных закономерностей.

Машинное обучение – это алгоритмы анализа данных, способствующие поиску в представленной информации закономерностей. При этом используются методы нейросетей, статистики, исследования операций и т. п. для выявления скрытой полезной информации в данных; при этом явно не программируются инструкции, указывающие, где искать данные и как делать выводы.

Элементами данного программного решения, по сути, его можно и назвать искусственным интеллектом следственных действий, должны быть:

- фундаментальные знания математики, линейной алгебры, теории вероятностей, статистики, информационных технологий, языков программирования (LISP, Python, Java, SQL, PHP, Swift, Kotlin, C/C++, Go);
- технологии интеллектуальной идентификации, технологии распознавания лица, включающие признаки Хаара, 68-и антропометрических точек и подобные другие;
- все известные голосовые программы, программы имитаторы голоса (Deepfake – созданные на базе нейронных сетей копий лиц и голосов);
- все известные алгоритмы, коды программирования, программы декодирования данных. Так как хакеры, как правило, используют разные диалекты кодирования для разных проектов;
- известные «цифровые» следы как способы и как конкретные преступные, уже совершенные деяния;
- типы, модели, компьютерные алгоритмы функционирования нейросетей, в том числе самообучающихся. Считается, что нейросеть – это один из методов машинного обучения; математическая модель, а также ее программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. В общем случае искусственная нейронная сеть (ИНС) может состоять из нескольких слоев простейших процессоров (нейронов), каждый из которых осуществляет некоторое математическое преобразование (вычисляет результат математической функции) над входными данными и передает полученный результат на следующий слой или на выход сети;
- компьютерное зрение, способное обрабатывать дактилоскопические базы, фотоматериалы, документальную информацию, личные дела сотрудников правоохранительного органа. С использованием нейросетей в компьютерном зрении можно выявлять от 92 до 99 % всех дефектов в зависимости от задачи, при ложных срабатываниях – на уровне 3–4 %. Современные системы видеоаналитики могут выявлять потенциально опасные ситуации. Среди основных сценариев работы видеоаналитики, например, контроль наличия средств индивидуальной защиты (каски, страховочные тросы, халаты, наушники) и доступа в опасные зоны;
- методы предиктивного анализа анализируют текущие и исторические данные, используя методы из статистики, интеллектуального анализа дан-

ных, машинное обучение и искусственный интеллект для того, чтобы делать прогнозы о будущем;

• интеграция с отдельными разработками российских разработчиков, таких как:

• проект ученых Нижегородского университета им. Лобачевского «ФОРВЕР», позволяющий формировать наиболее перспективные версии о личности преступника;

• система «Блок», обеспечивающая информационное криминалистическое сопровождение расследования экономических преступлений;

• система «Маньяк», обеспечивающая получение информации при расследовании серийных убийств на сексуальной почве;

• система «Спрут», помогающая установить контактные связи преступников;

• система «Сейф», в которой систематизируется информация о хищениях денежных средств из хранилищ;

• система мониторинга трафика компании NtechLab;

• географическая информационная система «Зеркало», оперирующая пространственными (фактографическими и статистическими) данными, и др.

Но надо понимать, что указанные базы данных и программные комплексы основаны на «нисходящем» подходе к пониманию искусственного интеллекта, поскольку ориентированы на решение либо одной конкретной задачи, либо группы однородных задач [5].

Предполагается, что создаваемая искусственная интеллектуальная система будет способствовать автоматизации данных, повышению производительности оперативно-розыскных действий, принятию процессуальных решений в рамках правоохранительного органа, персонализации преступлений, сокращению фактических сроков расследования, снижению как преступлений мошенничества, так и других квалификаций.

Согласно данным Министерства экономического развития Российской Федерации, сейчас реализуются возможности современных технологий искусственного интеллекта по следующим направлениям:

• компьютерному зрению (оно опирается на распознавание шаблонов и на глубокое обучение для распознавания изображений и видео. Машины уже умеют обрабатывать, анализировать и понимать изображения, а также снимать фото или видео и интерпретировать окружающую обстановку);

• обработке естественного языка (это способность компьютеров анализировать, понимать и синтезировать человеческий язык, включая устную речь. Используя Siri или Google assistant, уже можно управлять компьютерами с помощью обычного языка, используемого в повседневном обиходе.);

• распознаванию и синтезу речи;

• интеллектуальным системам поддержки принятия решений (ИСППР) (инструментарий выработки рекомендаций для лица, принимающего решение. Алгоритмы упорядочивают (ранжируют) конечное множество альтернатив (решений) или оптимизируют их на бесконечном множестве, используя технологии датамайнинга, моделирования и визуализации).

По данным, опубликованным на сайте Научно-технического центра ФГУР «ГРЧЦ», рынок данных услуг в России имеет тенденцию роста. По отношению к 2018 г., в 2023 г. он может вырасти в 4,8 раза, что составит 38 млрд рублей. Ключевые игроки на этом рынке сосредоточены на стратегическом партнерстве, приобретениях и выпусках новых продуктов для увеличения доходов. Примером является подписанное 9 ноября 2019 г. соглашение об альянсе Mail.ru Group, Сбербанк, Яндекс, Газпром нефть, МТС и РФПИ с целью реализации национальной стратегии развития искусственного интеллекта.

Уже сейчас при определенных законодательных инициативах, которые синхронизируются с Указом Президента Российской Федерации № 490 от 11.10.2019 г. «О развитии искусственного интеллекта в Российской Федерации», с инициативой Центрального Банка РФ по созданию национальной цифровой платформы для сбора, обработки и хранения биометрических персональных данных и отчасти уже реализованы для ГИБДД в системах мониторинга транспорта, можно предоставить правоохранительным органам доступ к программе регистрации СИМ-карт на базовых станциях мобильных операторов с целью отслеживания передвижения предполагаемых преступников [6].

Построение подобной структуры полностью увязывается с программой «Цифровая экономика России» по направлению «Цифровая инфраструктура», в которой предполагается развитие ряда технологических платформ 6-го технологического уклада, таких как:

• SafeNet (технологии комплексной безопасности инфокоммуникационных сетей),

• AeroNet (технологии беспилотных воздушных сетевых комплексов),

• EnergyNet (технологии интеллектуальных энергетических сетей),

• InfoNet (технологии информационных сетей),

• InnoNet (технологии сетевых нововведений – просьюмеринга, пиринговых и викисообществ научного и инженерного самоопределения в функции концептуальных единиц цифровой среды антропопрактик новой, приходящей парадигмы развития) [7].

Если начать сейчас построение правоохранительной цифровой архитектуры, первые практические результаты работающей как единое целое системы будут получены не ранее 2027 г.

## Список литературы

1. Борьба с мошенничеством с помощью искусственного интеллекта. URL: https://calmins.com/borba-s-moshennichestvom-s-pomoshhyu-iskusstvennogo-intellekta
2. Мошенничество в сети: судебная практика и ключевые аспекты. URL: https://rtmtech.ru/research/online-fraud-research
3. Искусственный интеллект: технологии и применение // Научно-технический центр ФГУП «ГРЧЦ». URL: https://rdc.grfc.ru/2020/12/aitech
4. Бахтеев Д.В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–6. URL: https://www.elibrary.ru/item.asp?id=43855502
5. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya
6. Указ Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: http://www.kremlin.ru/acts/bank/44731
7. Концепция глокально-интегрированной инфраструктуры пространственно-территориального развития как основа Генеральной схемы развития сетей связи Российской Федерации в рамках плана мероприятий по направлению «Информационная инфраструктура» программы «Цифровая экономика Российской Федерации» / С.А. Попов [и др.] // Физика волновых процессов и радиотехнические системы. 2019. Т. 22, № 1. С. 67–79. DOI: https://doi.org/10.18469/1810-3189.2019.22.1.67-79

## Информация об авторах

**Клюев Дмитрий Сергеевич**, доктор физико-математических наук, профессор, заведующий кафедрой радиоэлектронных систем Поволжского государственного университета телекоммуникаций и информатики, г. Самара, Россия. Автор более 250 научных работ.

*Область научных интересов*: электродинамика, устройства СВЧ, антенны, метаматериалы.

*E-mail*: klyuevd@yandex.ru

*ORCID*: https://orcid.org/0000-0002-9125-7076

**Смушкин Александр Борисович**, кандидат юридических наук, доцент кафедры уголовного права и процесса Поволжского института (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), г. Саратов, Россия.

*Область научных интересов*: цифровая криминалистика, цифровизация, цифровая трансформация расследования, электронное правосудие, информационные технологии в расследовании.

*E-mail*: skif32@yandex.ru

*ORCID*: https://orcid.org/0000-0003-1619-8325

**Соколова Юлия Владимировна**, кандидат физико-математических наук, доцент, доцент кафедры радиоэлектронных систем Поволжского государственного университета телекоммуникаций и информатики, г. Самара, Россия.

*Область научных интересов*: электродинамика, устройства СВЧ, антенны, метаматериалы.

*E-mail*: ula.81.81@mail.ru

*ORCID*: https://orcid.org/0000-0003-2873-8675

**Платонов Сергей Евгеньевич**, младший судебный пристав по обеспечению установленного порядка деятельности судов специализированного отделения по обеспечению установленного порядка деятельности Шестого кассационного суда общей юрисдикции Российской Федерации Главного управления Федеральной службы судебных приставов России по Самарской области, прапорщик внутренней службы, магистрант Поволжского института (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), г. Саратов, Россия.

*Область научных интересов*: криминалистика, информационные технологии, методика следственных действий.

*E-mail*: platonovse@mail.ru

Physics of Wave Processes and Radio Systems
*2023, vol. 26, no. 3, pp. 116–122*

DOI 10.18469/1810-3189.2023.26.3.116-122
UDC 343.9
Original Research

*Received* 13 December 2022
*Accepted* 17 January 2023
*Published* 27 September 2023

# Analysis of the possibilities of artificial intelligence for investigation of fraud

*Dmitriy S. Klyuev*[1], *Alexander B. Smushkin*[2], *Yulia V. Sokolova*[1], *Sergey E. Platonov*[2]

[1] Povolzhskiy State University of Telecommunications and Informatics
23, L. Tolstoy Street,
Samara, 443010, Russia
[2] Povolzhskiy Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia)
55, Radishchev A.N. Street,
Saratov, 410003, Russia

*Abstract* – **Background.** As a result of the digitalization of society, the number of fraudulent activities using information and telecommunication technologies is growing. The technological complexity of the investigation is such that it requires the use of similar tools in investigative and operational-search activities. Such tools can be artificial intelligence. **Aim.** Determine the potential of artificial intelligence in investigative and operational activities. **Methods.** The analysis method was used to evaluate existing solutions for use in investigative and operational activities, such as face recognition, based on Haar rules, imitator programs and voice control, solutions of the Incident Management service, Papillon AFIS, Zerkalo GIS, Forver project, IS «Obraz++», machine learning capabilities, neural networks. **Results.** Some relevant solutions are shown that require integration into a single system of technological and intelligent solutions (artificial intelligence) for investigative actions and operational-search activities. **Conclusion.** Presented are modern automated information tools that require their integration into a single intelligent technological system (artificial intelligence) for investigating crimes.

*Keywords* – investigative actions; classical and digital fraud; machine learning; neural networks; digital footprints; intelligent identification; artificial intelligence.

platonovse@mail.ru (*Sergey E. Platonov*)



## References

1. "Fight against fraud with the help of artificial intelligence." [Online.] Available: https://calmins.com/borba-s-moshennichestvom-s-pomoshhyu-iskusstvennogo-intellekta (In Russ.)
2. "Online fraud: jurisprudence and key aspects." [Online.] Available: https://rtmtech.ru/research/online-fraud-research (In Russ.)
3. "Artificial intelligence: technologies and applications." Scientific and technical center of the Federal State Unitary Enterprise «GRC». [Online.] Available: https://rdc.grfc.ru/2020/12/aitech (In Russ.)
4. D. V. Bakhteev, "Artificial intelligence in investigative activities: tasks and problems," *Rossiyskiy sledovatel'*, no. 9, pp. 3–6, 2020, url: https://www.elibrary.ru/item.asp?id=43855502. (In Russ.)
5. D. V. Bakhteev, "Artificial intelligence in forensics: state and prospects for use," *Ugolovnyy protsess i kriminalistika*, no. 2, pp. 43–49, 2018, url: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-kriminalistike-sostoyanie-i-perspektivy-ispolzovaniya. (In Russ.)
6. Decree of the President of the Russian Federation of October 10, 2019, no. 490 «On the development of artificial intelligence in the Russian Federation», url: http://www.kremlin.ru/acts/bank/44731. (In Russ.)
7. S. A. Popov et al., "The concept of a glocal-integrated infrastructure of spatial and territorial development as the basis of the General scheme for the development of communication networks of the Russian Federation in the framework of the action plan for the «Information infrastructure» program of the «Digital economy of the Russian Federation»," *Physics of Wave Processes and Radio Systems*, vol. 22, no. 1, pp. 67–79, 2019, doi: https://doi.org/10.18469/1810-3189.2019.22.1.67-79. (In Russ.)

## Information about the Authors

**Dmitriy S. Klyuev**, Physical and Mathematical Sciences Doctor, Radioelectronic Systems Department Head, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia. Author of over 250 scientific papers.
*Research interests*: electrodynamics, microwave devices, antennas, metamaterials.
*E-mail*: klyuevd@yandex.ru
*ORCID*: https://orcid.org/0000-0002-9125-7076

**Alexander B. Smushkin**, Candidate of Legal Sciences, associate professor of the Department of Criminal Law and Procedure, Povolzhskiy Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Saratov, Russia.

*Research interests*: digital forensics, digitalization, digital transformation of investigation, e-justice, information technologies in investigation.
*E-mail*: skif32@yandex.ru
*ORCID*: https://orcid.org/0000-0003-1619-8325

**Yulia V. Sokolova**, Physical and Mathematical Sciences Candidate, Radioelectronic Systems Department Associate Professor, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russia.
*Research interests*: electrodynamics, microwave devices, antennas, metamaterials.
*E-mail*: ula.81.81@mail.ru
*ORCID*: https://orcid.org/0000-0003-2873-8675

**Sergey E. Platonov**, junior bailiff for ensuring the established procedure for the activities of the courts of the specialized department for ensuring the established procedure for the activities of the Sixth Cassation Court of General Jurisdiction of the Russian Federation of the Main Directorate of the Federal Bailiffs Service of Russia for the Samara Region, ensign of the internal service, undergraduate of the Povolzhskiy Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Saratov, Russia.
*Research interests*: forensic science, information technology, investigative methodology.
*E-mail*: platonovse@mail.ru