

Дата поступления рукописи в редакцию: 12.05.2026 г.

DOI: 10.24412/2076-1503-2026-6-563-567

Дата принятия рукописи в печать: 29.06.2026 г.

ПЕТРОВА Наталья Дмитриевна,
кандидат юридических наук,
доцент кафедры общетеоретических правовых дисциплин
СЗФ ФГБОУВО «РГУП им. В.М. Лебедева», Санкт-Петербург, Россия,
e-mail: nava2009@yandex.ru

СУДАРЬКОВА Ксения Валерьевна,
студент 2 курса специалитета
СЗФ ФГБОУВО «РГУП им. В.М. Лебедева», Санкт-Петербург, Россия,
e-mail: kseniasudarkova@gmail.com

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ИИ-СИСТЕМ ДЛЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ: ОТ РАСПОЗНАВАНИЯ ЛИЦ ДО ПРЕДИКТИВНОЙ АНАЛИТИКИ

Аннотация. В эпоху цифровизации правоохранительные органы всё чаще нуждаются в системах для быстрого анализа данных, поиска и сопоставления фактов, выявления закономерностей и ускорения расследований. Подобные инструменты применялись и раньше, первые автоматизированные решения появились ещё в советский период. Нынешнее поколение ии-систем представляет собой интегрированные платформы с функциями предиктивной аналитики и биометрического сопоставления. С учётом современных тенденций разрабатываются новые решения для противодействия кибермошенничеству, прогнозирования угроз, борьбы с дипфейками и фишинговыми сайтами. Хотя их внедрение осложняется техническими ошибками алгоритмов, правовыми пробелами, рисками утечек данных и высокой стоимостью внедрения, они остаются важным и эффективным «помощником» для правоохранителей.

Ключевые слова: искусственный интеллект, программное обеспечение, идентификация, предикативная аналитика.

PETROVA Natalya Dmitrievna,
Candidate of Law, Associate Professor,
Department of General Theoretical Legal Disciplines,
NWF FGBOUVO "RGUP named after V.M. Lebedev",
St. Petersburg, Russia

SUDARKOVA Ksenia Valerievna,
2nd year specialist student NWF FGBOUVO
"RGUP named after V.M. Lebedev", St. Petersburg, Russia

EFFECTIVENESS OF USING AI-SYSTEMS FOR LAW ENFORCEMENT IN RUSSIA: FROM FACIAL RECOGNITION TO PREDICTIVE ANALYTICS

Annotation. In the era of digitalization, law enforcement agencies are increasingly in need of systems for rapid data analysis, fact retrieval and matching, pattern detection, and acceleration of investigations. Such tools have been used before, with the first automated solutions appearing during the Soviet period. The current generation of AI systems is an integrated platform with predictive analytics and biometric matching capabilities. In line with current trends, new solutions are being developed to combat cyber fraud, predict threats, and combat deepfakes and phishing websites. Although their implementation is complicated by technical errors in algorithms, legal gaps, risks of data leaks, and high implementation costs, they remain an important and effective "assistant" for law enforcement agencies.

Key words: artificial intelligence, software, identification, predictive analytics.

Использовать в криминалистике системы, которые помогали хранить и анализировать данные начали ещё в Советском Союзе. Постепенно, с развитием технологий и возможностей их использования появились первые масштабные системы контроля и использованием ИИ - видеонаблюдение с распознаванием лиц и анализом данных о возможных правонарушениях. На данный момент разработаны системы, главная цель которых ускорить расследование, повысить точность выявления преступлений и оптимизировать работу сотрудников правоохранительных органов, а именно системы предиктивной аналитики, цифровой криминалистики и борьбы с дипфейками.

В работе мы рассмотрим путь развития ИИ-систем, основные направления их применения, перспективы их развития и проблемы применения на практике.

В российских регионах системы камер наблюдения стали активно появляться с середины 1990-х годов. Первоначально они пользовались популярностью в частном секторе, но ко второй половине 2000-х годов их взяли на вооружение правоохранительные органы [1]. Одним из первых крупных городов, в котором была установлена система видеонаблюдения «Безопасный город» стала Москва в 2006 году [2]. Такая система была установлена и в других городах, но они были локальными и не интегрировали между ведомствами. Качество разрешения было низким и никакими аналитическими функциями система также не обладала. К 2010-2015 годам постепенно был совершён переход к цифровому видеонаблюдению, начали создавать единые центры мониторинга, появились IP-камеры с высоким разрешением, что улучшило качество изображения и позволило внедрить технологию распознавания лиц. Успешно прошла тест программа в 2017 году (конечно же в Москве) на Кубке конфедераций по футболу на болельщиках. Постепенно подобную технологию начали использовать в метрополитене и других городах (Калининград, Екатеринбург, Казань, Воронеж, Новороссийск и другие), а некоторые создали свои собственные системы (Санкт-Петербург: комплекс «Городовой» - осуществляет контроль благоустройства, выявления возможные признаки хулиганства; Новосибирская область: сервис для розыска пропавших детей через «Безопасный город»; Татарстан: проект «Урам» для поиска бездомных и людей в трудной ситуации).

В 2020 году был введён полицейский блок распознавания лиц «Парсив» - это шлюз, через который полицейские могут подключаться к городской системе распознавания лиц. Система позволяет сопоставлять съёмки этого же человека с другими камерами наблюдения на конкретном

участке, что позволяет проследить за его передвижениями. Из-за пандемии COVID-19 властям пришлось начать использовать блок ранее (чтобы отслеживать нарушения режима самоизоляции), чем это было запланировано изначально. Результатом этого стала отправка в 2021 году системы на доработку подрядчику из Перми «Брайт софт» на сумму 236 млн руб [3]. Правда, результатов этих «доработок» пока что увидеть не удалось, хотя подрядчику и было выделено 440 дней, начиная с 1 октября 2021 года.

Развитие систем видеонаблюдения в России прошло значительный путь от локальных частных решений 1990-х годов до современных интегрированных систем с функцией распознавания лиц. «Безопасный город» стал хорошей основой для создания новых инструментов и ресурсов по интеграции, защите информации и регламентации процессов для перехода к «умным решениям» [4]. Система продолжает развиваться, только в Петербурге насчитывается около 113 тысяч камер и их количество продолжает расти не только здесь, но и в других городах. Внедрение аналитических систем существенно повышает эффективность работы правоохранительных органов и уровень общественной безопасности, что делает их развитие приоритетным направлением в сфере городского видеонаблюдения. Несмотря на значительные достижения, система требует дальнейшей доработки, для повышения точности и эффективности работы.

Рассматривая другие системы, важно отметить, что подробной информации о способах и принципах работы, алгоритмах, используемых данных и статистики пользования в открытом доступе нет. Для широкого круга доступна только достаточно поверхностная информация о целях и перспективах работы систем. В остальном для изучения приходится полагаться на сетевые издания, комментарии разработчиков и других специалистов. При чём найти данные от людей, которые напрямую связаны с созданием и работой систем достаточно сложно, а даже если они есть, то никаких подробностей они не содержат. Так что при анализе систем мы будем опираться на доступные массовому пользователю данные, т.к. иные нам недоступны.

Одной из первых систем, о которой следует упомянуть, является система обеспечения безопасности «Маньяк». Основное ее предназначение – реализовать порядок и отсутствие преступных деяний во время проведения Олимпиады 80-х в Москве [5]. В основе принципа работы системы лежит внесение в специальную таблицу данных – характеристик с места преступления, которые впоследствии анализируются искусственным интеллектом, и следователю предлагается наиболее верный вариант в качестве версии [6].

Главная цель - составить психолого-криминалогический портрет предполагаемого преступника и найти закономерности в разрозненных преступлениях, совершённого одним человеком.

По словам экспертов, благодаря этой системе удалось поймать «ангарского маньяка» Михаила Попкова, совершившего более 80 убийств в Иркутской области в период с 1992 по 2011 год.

Автоматизированная информационная система (АИС) «Сейф» была разработана в 1990-х годах. Она начала функционировать с 1 января 1990 года, так как учёт хищений из металлических хранилищ (сейфов, шкафов, ящиков) в этой системе формировался из информационных карт на преступление, зарегистрированных по линии уголовного розыска с этой даты. Система «Сейф» представляет собой базу данных краж из хранилищ (в первую очередь, банковских) и сейфов, принадлежащих компаниям и гражданам. В «Сейфе» по данным Анны Голуб (юрист фирмы Criminal Defense Firm) информация о преступлениях и их характеристиках (способах и инструментах взлома, предметах преступления) хранится в виде карточек. Основа работы данного ПО по уточнению Антона Шустикова – предиктивная аналитика, которая позволяет правоохранительным органам объединять преступления в серии и направлять патрули в наиболее уязвимые точки в нужное время.

Российское ПО «Спрут» помогает выявлять организованную преступность: на основе знаний о преступных формированиях, о связи лиц, представляющих оперативный интерес, о экономических криминогенных факторах, устанавливает связи между преступниками.

Экспертная система «Блок», в свою очередь, помогает установить возможные способы совершения хищений при проведении строительных работ.

Программное обеспечение «Мобильный Криминалист» помогает значительно ускорить процесс изучения цифровых доказательств.

ПО извлекает и анализирует данные с телефонов, планшетов, ПК и облачных сервисов. Это необходимо для сбора цифровых улик, предотвращения утечек данных и выявления уязвимостей локальных систем. Поддерживает более 40 000 моделей устройств на разных операционных системах.

Программное обеспечение обладает тремя ключевыми функциями:

Распознавание текста с различных визуальных носителей (фотографии, скриншоты) с поддержкой множества языков и высокой точностью обработки.

Идентификация лиц на фото и видеоматериалах, включая анализ характерных черт при различных условиях съёмки (углы, освещение). Система автоматически сопоставляет новые лица с уже имеющимися в базе данными.

Преобразование речи в текстовый формат, осуществляемое путём обработки аудио и видеофайлов с последующим переводом голосовых записей в письменный текст [7].

«Криминалист» — комплексная система, которая объединяет данные из баз МВД, ФСБ, СКР, ФНС, Росфинмониторинга и других ведомств, а также из открытых источников (соцсети, СМИ). Она выявляет потенциальных преступников, группировки, места совершения преступлений и предлагает оптимальные решения для правоохранителей. В 2020 году в России был задержан подозреваемый в хищении бюджетных средств благодаря системе «Криминалист», которая выявила его связи с другими фигурантами дела [8].

Федеральная информационная система биометрических учётов (ФИСБУ) использует камеры видеонаблюдения для поиска подозреваемых в совершении преступлений, как на стадии сбора информации, так и последующей обработки [9]. Эти данные позволяют распознавать людей не только по изображению их лиц, но и сравнивать голос, радужную оболочку глаз, татуировки, а также иные имеющиеся у людей идентифицирующие признаки. В настоящее время основное регулирование биометрических данных в России осуществляется через Единую биометрическую систему и регулируется Федеральным законом от 29 декабря 2022 года №572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных».

К январю 2026 года в системе зарегистрировалось около 9 млн человек с темпом до 20 тыс. регистраций в сутки. С 1 апреля 2026 года ФСБ получила прямой доступ к базам данных организаций [10].

Перейдём к системам, которые пока только разрабатываются нашими программистами. Информации о них ещё меньше, чем о системах, которые уже выпущены и используются правоохранительными органами, поэтому в описаниях будет содержаться только краткая информация о целях и планируемых датах запуска.

Следует также упомянуть такие системы, как «Клон» - система для выявления поддельных видео, включая дипфейки, а также «Конъюнктуру» — систему прогнозирования чрезвычайных ситуаций и моделирования сценариев реагирования на них. [11]. Обе системы планировались к запуску в 2025 году в рамках плана МВД по внедрению

ИИ. Однако в открытых источниках нет информации о фактическом запуске этих систем в эксплуатацию. Возможно, сроки были перенесены или проект претерпел изменения.

Правительством РФ была утверждена программа по созданию ИИ-алгоритма обнаружения случаев кибермошенничества – распоряжение Правительства РФ от 14 августа 2025 года №2207-р «О плане мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно – коммуникационных технологий» для борьбы с фишинговыми сайтами и мошенническими звонками с подделкой голосов. Проект курируют Минцифры, МВД и Роскомнадзор. Работа по созданию и запуску системы должна закончиться в первом квартале 2028 года.

Помимо этого, в третьем квартале 2026 года планируется запуск единого реестра официальных сайтов интернет – магазинов. [12].

Развитие ИИ-систем в правоохранительной деятельности прошло путь от первых автоматизированных решений до современных комплексных платформ с элементами предиктивной аналитики и биометрической идентификации.

На ранних этапах системы помогали накапливать и структурировать криминалистические данные и анализировать их, а позже, с развитием технологий, стало доступно и распознавание лиц с биометрическим учётом. Постепенно, возможности только расширялись и распознавание велось не только по лицу, но и по голосу, радужной оболочке глаз и другим признакам. Комплексные аналитические платформы, такие как «Криминалист» и «Мобильный Криминалист», объединили данные межведомственных структур и открытых источников, ускорив анализ цифровых улик.

Вместе с тем обозначился и ряд проблем, среди которых проблема программирования ИИ (среди которых ошибки алгоритмов и самих специалистов), результаты и выводы, сделанные ИИ (невозможность интерпретации языка и чувств, которые понятны лишь человеку), вопрос автоматизации и бесконтрольности со стороны человека робототехнических устройств [13, с. 21].

Существуют пробелы в законодательстве, а также отсутствует система нормативных актов, которая четко и логично была выверена, а также ИИ-системы не закреплены в праве как субъект и не имеют правового статуса.

Также, масштабное использование биометрии и видеонаблюдения ставит под сомнения вопросы приватности и защиты данных населения, что, конечно, вызывает недовольство граждан. Создание ЕБС не поддерживают 50% опрошенных, 19% уже разместили там свои данные,

больше трети респондентов о возможности сдать биометрию слышат впервые, следует из опроса НАФИ, который проводился в октябре среди 1,6 тысячи жителей 53 российских субъектов в 2020 году. Опасения людей связаны прежде всего с возможностью утечки данных, что небезосновательно: так из базы «Новгородского клинического специализированного центра физиопульмонологии» были предоставлены на продажу персональные данные людей, больных туберкулезом, была «слита» база участников и партнёров конкурса «Лидеры России», в Москве и Подмосковье в свободном доступе имеются личные данные около миллиона водителей [14].

ИИ-системы стали неотъемлемой частью правоохранительной деятельности в России. Они заметно ускоряют расследования и оптимизируют работу органов. Для стабильно развития необходимо решить проблемы прозрачности, технической надёжности и правовой регламентации, обеспечивая баланс между общественной безопасностью и защитой прав граждан, с помощью повышения доверия к системам и повышения уровня безопасности хранения конфиденциальных данных.

Список литературы:

- [1] Серебренников Д.Е. Gaze Ex Machina: Краткая история систем полицейского видеонаблюдения в России и за рубежом // Городские исследования и практики. 2023. №3. URL: <https://cyberleninka.ru/article/n/gaze-ex-machina-kratkaya-istoriya-sistem-politseyskogo-videonablyudeniya-v-rossii-i-za-rubezhom> (дата обращения: 31.03.2026).
- [2] Москве будет безопаснее // Connect! Мир связи. — 2006. — № 3. — С. 45–48.
- [3] Большой брат в Москве: создаётся система тотальной видеослежки за жителями // kprf121.ru. URL: <https://kprf121.ru/bolshoj-brat-v-moskve-sozdaetsya-sistema-totalnoj-videoslezhki-za-zhitelyami/> (дата обращения: 01.03.2026)
- [4] «Безопасный город» // Официальный портал Администрации Санкт-Петербурга. URL: https://www.gov.spb.ru/gov/otrasl/c_information/napravlenie-deyatelnosti-komiteta/bezopasnyj-gorod/ (дата обращения: 01.03.2026).
- [5] Большой брат: как технологии следят за нами // Incrussia. — 2026. URL: https://incrussia.ru/understand/bolshoy_brat/?ysclid=mnn2j2p_woc219479970 (дата обращения: 06.04.2026).
- [6] Иванов А.А. Судебная практика по делам о защите чести и достоинства // Право.ру. URL: <https://pravo.ru/story/254219/> (дата обращения: 06.04.2026).
- [7] Искусственный интеллект в цифровой криминалистике: возможности и будущее // МКО

Systems. URL: <https://docs.mko-systems.ru/blog/artificial-intelligence-digital-forensics?ysclid=moiq59fcc4616623135> (дата обращения: 28.04.2026).

[8] Светункова А. Нейронное дело: как ИИ помогает в борьбе с преступностью // iz.ru. URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu> (дата обращения: 28.04.2026).

[9] Информационная система биометрических учётов (ФИСБУ) // URL: <https://www.tadviser.ru/index.php> (дата обращения: 21.03.2026).

[10] Биометрия и ответственность бизнеса: штрафы до 500 млн рублей и уголовная статья в 2026 году // Vitvet.com. URL: <https://vitvet.com/about/news/biometricheskie-dannye-biznes-shtraf-ebs-2026/> (дата обращения: 30.04.2026).

[11] МВД планирует использовать нейросети для поиска видеоподделок и прогнозирования ЧС // Rozetked.me. URL: <https://rozetked.me/news/31967-mvd-planiruet-ispol-zovat-neyroseti-dlya-poiska-videopoddelok-i-prognozirovaniya-chs> (дата обращения: 30.04.2026).

[12] Нейросети на страже порядка: как ИИ меняет работу полиции // РБК Компании. URL: <https://companies.rbc.ru/news/SoVgLUyJhB/nejroseti-na-strazhe-poryadka-kak-ii-menyaet-rabotu-politsii/> (дата обращения: 30.04.2026).

[13] Агеев В.В. Большие данные и искусственный интеллект на службе полиции // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сб. ст. междунар. науч.-практ. конф., Москва, 30 октября 2019 г. / отв. за выпуск В.О. Лапин. – М.: Академия управления Министерства внутренних дел Российской Федерации, 2019.

[14] Он и тебя сосчитал: почему россияне не доверяют биометрии // News.ru. URL: <https://news.ru/investigations/on-i-tebya-soschital-pochemu-rossiyane-ne-doverayut-biometrii?ysclid=mokpyz8r74443154836> (дата обращения: 30.04.2026).

References:

[1] Serebrennikov D.E. Gaze Ex Machina: A Brief History of Police Video Surveillance Systems in Russia and Abroad // Urban Research and Practices. 2023. No. 3. URL: <https://cyberleninka.ru/article/n/gaze-ex-machina-kratkaya-istoriya-sistem-politseyskogo-videonablyudeniya-v-rossii-i-za-rubezhom> (accessed: 31.03.2026).

[2] Moscow Will Be Safer // Connect! The World of Communications. - 2006. - No. 3. - Pp. 45-48.

[3] Big Brother in Moscow: A System of Total Video Surveillance of Residents is Being Created // kprf121.ru. URL: <https://kprf121.ru/bolshoj-brat-v-moskve-sozdaetsya-sistema-totalnoj-videoslezhki-za-zhitelyami/> (Accessed: 01.03.2026)

[4] "Safe City" // Official Portal of the Saint Petersburg Administration. URL: https://www.gov.spb.ru/gov/otrasl/c_information/napravlenie-deyatelnosti-komiteta/bezopasnyj-gorod/ (Accessed: 01.03.2026).

[5] Big Brother: How Technologies Spy on Us // Incrussia. - 2026. URL: <https://incrussia.ru/understand/bolshoy-brat/?ysclid=mn2j2pwoc219479970> (Accessed: 06.04.2026).

[6] Ivanov, A.A. "Court Practice in Cases of Protection of Honor and Dignity" // Pravo.ru. URL: <https://pravo.ru/story/254219/> (accessed on April 6, 2026).

[7] Artificial Intelligence in Digital Forensics: Possibilities and the Future // MKO Systems. URL: <https://docs.mko-systems.ru/blog/artificial-intelligence-digital-forensics?ysclid=moiq59fcc4616623135> (accessed on April 28, 2026).

[8] Svetunkova, A. "Neural Matter: How AI Helps in the Fight Against Crime" // iz.ru. URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu> (accessed on April 28, 2026).

[9] Biometric Accounting Information System (BIAS) // URL: <https://www.tadviser.ru/index.php> (accessed on March 21, 2026).

[10] Biometrics and Business Responsibility: Fines of Up to 500 Million Rubles and a Criminal Code in 2026 // Vitvet.com. URL: <https://vitvet.com/about/news/biometricheskie-dannye-biznes-shtraf-ebs-2026/> (accessed on April 30, 2026).

[11] The Ministry of Internal Affairs plans to use neural networks to detect video fakes and predict emergencies // Rozetked.me. URL: <https://rozetked.me/news/31967-mvd-planiruet-ispol-zovat-neyroseti-dlya-poiska-videopoddelok-i-prognozirovaniya-chs> (date of access: 30.04.2026).

[12] Neural networks guarding order: how AI is changing the work of the police // RBC Companies. URL: <https://companies.rbc.ru/news/SoVgLUyJhB/nejroseti-na-strazhe-poryadka-kak-ii-menyaet-rabotu-politsii/> (date of access: 30.04.2026).

[13] Ageyev V.V. Big Data and Artificial Intelligence in the Service of the Police // Strategic Development of the System of the Ministry of Internal Affairs of Russia: Status, Trends, Prospects: Coll. Art. of the International Scientific and Practical Conf., Moscow, October 30, 2019 / V.O. Lapin, responsible for the issue. – Moscow: Academy of Management of the Ministry of Internal Affairs of the Russian Federation, 2019.

[14] He Counted You, Too: Why Russians Don't Trust Biometrics // News.ru. URL: <https://news.ru/investigations/on-i-tebya-soschital-pochemu-rossiyane-ne-doverayut-biometrii?ysclid=mokpyz8r74443154836> (accessed: April 30, 2026).