УДК 34

Использование цифровых технологий с искусственным интеллектом в борьбе с киберпреступностью в России и зарубежом

Сираканян Аркадий Рашимович

Кандидат юридических наук,
заместитель директора Института государства и права
Сургутского государственного университета,
628412, Российская Федерация, Сургут, просп. Ленина, 1;
e-mail: Sirakanyan_ar@surgu.ru

Аннотация

В статье исследуются современные методы применения цифровых технологий и искусственного интеллекта для противодействия киберпреступности в России и зарубежом. Рассматриваются ключевые инструменты, используемые правоохранительными органами, включая системы анализа больших данных, распознавания образов и предиктивной аналитики. Анализируются преимущества искусственного интеллекта, включая скорость обработки информации и автоматизацию рутинных задач, а также проблемы, связанные с ошибками алгоритмов, вопросами конфиденциальности и необходимостью правового регулирования. В статье приводятся мнения ученых относительно использования цифровых технологий со встроенным интеллектом и дается авторское мнение по данному вопросу. Приводятся примеры реальных кейсов, где технологии помогли раскрыть преступления, и обсуждаются перспективы развития ИИ-инструментов в контексте национальной кибербезопасности. Статья предназначена для специалистов в области цифровой криминалистики, правоохранительных органов и всех, кто интересуется технологическими аспектами борьбы с киберпреступностью.

Для цитирования в научных исследованиях

Сираканян А.Р. Использование цифровых технологий с искусственным интеллектом в борьбе с киберпреступностью в России и зарубежом // Вопросы российского и международного права. 2025. Том 15. № 2А. С. 506-515.

Ключевые слова

Искусственный интеллект, киберпреступность, криминалистика, анализ больших данных, машинное обучение, российские ИИ-технологии.

Введение

В условиях стремительной цифровизации общества киберпреступность становится одной из ключевых угроз национальной безопасности. Традиционные методы борьбы с цифровыми преступлениями зачастую оказываются недостаточно эффективными из-за высокой динамики развития атакующих технологий. В этой связи применение искусственного интеллекта (далее – ИИ) открывает новые возможности для обнаружения, предотвращения и расследования киберпреступлений. Все это обуславливает актуальность данной темы. В данной статье рассматриваются современные технологии на основе ИИ, применяемые в России для противодействия киберугрозам, анализируются их преимущества и ограничения, а также перспективы дальнейшего развития.

Основная часть

Чтобы проникнуться данной проблемой, необходимо вернуться к истокам, вспомнить о самом зарождении киберпреступности в России, которое началось в конце 1980-х – начале 1990-х годов, параллельно с развитием компьютерных технологий и распространением Интернета. В связи с этим необходимо выделить следующие этапы зарождения киберпреступности в России:

1. 1980-е – начало 1990-х годов. Первые хакеры. В СССР компьютерные технологии развивались в основном в научных и военных кругах, но с появлением персональных компьютеров (например, «Электроника БК-0010», ZX Spectrum) появились первые энтузиасты-программисты. В то же время создавались первые вирусы («Пентагона», «Вася»), но отметим, что они создавались скорее из любопытства, чем для преступных целей.

2. 1990-е годы. Расцвет хакерства и первые преступления. С распадом СССР и появлением коммерческих интернет-провайдеров (например, «Релком», «Демос») начали формироваться первые хакерские группы. Уже в этот период происходили взломы банковских систем, кража данных кредитных карт (например, группа хакеров из Санкт-Петербурга, взломавшая Citibank в 1994 году и похитившая $10 млн) [Подстава века или таинственная история взлома Ситибанка, www]

3. 2000-е годы. Профессионализация киберпреступности. С развитием Интернета и электронных платежей (WebMoney, Яндекс.Деньги) появились новые виды мошенничества: фишинг (создание поддельных сайтов для кражи данных); кардинг (торговля украденными данными карт); ботнеты (сети заражённых компьютеров для DDoS-атак и рассылки спама).

4. 2010-е годы – настоящее время.

По данным FBI Internet Crime Report [Internet Crime Complaint Center (IC3), www] за 2023-2024 годы, мировой ущерб от киберпреступлений превысил $23 млрд (рост на 40% с 2022 года). Interpol сообщает о +300% росте фишинговых атак с 2020 года. Самые частые преступления (по Verizon DBIR 2024): фишинг (35% атак), утечки данных из-за уязвимостей ПО (27%), Ransomware (атаки выросли на 45% в 2023).

Киберпреступность в России, как и во всем мире, демонстрирует устойчивый рост: по данным МВД РФ, количество преступлений в цифровой среде увеличивается на 15–20% ежегодно. В 2024 году в России зафиксированы 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Это составляет примерно 40% от общего числа противоправных деяний. Такие данные в конце января 2025 года обнародовало МВД РФ. В отчете ведомства говорится, что в 2024 году общее количество

киберпреступлений в России увеличилось на 13,1% по сравнению с предыдущим годом. При этом в ИТ-сфере совершены 369,3 тыс. тяжких и особо тяжких противоправных деяний, что на 7,8% больше в годовом исчислении. В значительной степени этот фактор повлиял на рост в 2024 году общего числа тяжких и особо тяжких преступлений на 4,8% [Статистика киберпреступности в российских регионах: данные МВД за 2024 год», www].

Основными угрозами остаются фишинг, DDoS-атаки, распространение вредоносного ПО, утечки персональных данных и атаки на критическую инфраструктуру.

Традиционные методы защиты, такие как сигнатурный анализ и правила-based системы, не справляются с новыми видами атак, требующими оперативного реагирования. Внедрение ИИ позволяет автоматизировать процессы обнаружения аномалий, прогнозирования угроз и принятия решений в реальном времени.

В настоящее время в России активно внедряются цифровые технологии с ИИ в борьбе киберпреступлениями. Разберем реальные кейсы от ПАО Сбер, Лаборатории Касперского, ПАО Ростелекома, МВД и ФСБ России, Роскомнадзора.

Сбербанк активно борется с мошенничеством через NLP и «киберград» [Открытая NLP-модель для классификации ESG-рисков, www]. NLP (Natural Language Processing, обработка естественного языка) – это направление ИИ, которое занимается взаимодействием компьютеров и человеческого языка. NLP позволяет машинам понимать, анализировать, генерировать и интерпретировать текстовую и устную речь. КиберГрад – это инновационная система защиты от киберугроз, разработанная Сбербанком на базе ИИ и машинного обучения (ML). Она предназначена для обнаружения и предотвращения мошеннических операций в реальном времени, а также анализа цифровых угроз. Например, по последней доступной статистике, Система «Киберград» на базе ИИ: анализирует более 1 млн операций ежедневно; снизила успешные мошеннические транзакции на 37% (2023); распознает голосовые фишинговые звонки (точность 92%). А с помощью ИИ на основе NLP для блокировки фишинга: в 2023 году выявлено 12,8 тыс. поддельных сайтов; автоматически блокирует более 90% SMS-сообщений с мошенническими ссылками.

Лаборатория Касперского активно применяет ИИ для обнаружения неизвестных угроз. Для этих целей был разработан Kaspersky MLAD (Machine Learning Anomaly Detection) [Kaspersky Machine Learning for Anomaly Detection, www] – это продвинутая система защиты от кибератак на основе машинного обучения (ML). Она предназначена для обнаружения сложных и ранее неизвестных угроз, которые не выявляются традиционными сигнатурными методами. По данным Лаборатории Касперского, данная система обнаруживает 65% новых вредоносных программ без сигнатур, а также используется в «КиберЩите Ростелекома» для защиты госучреждений. По доступной статистике за 2024 год, заблокировано 1,2 млн атак на российские компании, а также зафиксировано снижение ложных срабатываний на 40% по сравнению с традиционными методами.

ПАО Ростелеком также активно внедряет ИИ в свои системы. Киберзащита Ростелекома [Ростелеком усилил киберзащиту технологических процессов, www] – это комплекс технологических решений и сервисов, предоставляемых компанией ПАО «Ростелеком» (включая дочернюю структуру Solar Security) для обеспечения информационной безопасности государственных и коммерческих организаций России. Из основных направлений действия киберзащиты можно выделить:

1. Solar JSOC (Центр мониторинга и реагирования на кибератаки). Он обеспечивает круглосуточный мониторинг угроз. В 2024 году обработал свыше 1,5 млн инцидентов (данные

Solar Security).

2. Защита критической инфраструктуры (КИИ) посредством реализации требований 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации»: защита энергосистем (например, «Россети») и киберизоляция объектов ТЭК.

ФСБ и МВД в расследовании киберпреступлений используют Систему «Помор» – это разработанный ФСБ России программно-аналитический комплекс для мониторинга и противодействия киберугрозам, включая расследование преступлений в даркнете и противодействие терроризму. С помощью этой системы анализируются darknet-форумы и Telegram-каналы. За 2023-2024 годы эта система помогла обнаружить канал утечки данных из МФЦ (1,2 млн записей), ликвидировать DDoS-ботнет из 17 тыс. камер наблюдения, раскрыть схемы обнала через криптовалюты (на 4,3 млрд руб.).

Роскомнадзор использует ИИ для автоматической блокировки запрещенного контента с помощью ИИ-системы «Отис» [ЕСИА, www] – это разработанная Роскомнадзором автоматизированная платформа для мониторинга и блокировки запрещенного контента в Интернете с использованием ИИ. Система названа в честь Отиса – первого в мире робота-полицейского (из фантастического рассказа Айзека Азимова), что символизирует ее «надзорную» функцию. Данная система ежедневно проверяет более 200 тыс. интернет-страниц. По известным данным, в 2024 году заблокировала 320 тыс.

ресурсов с запрещенным контентом. Точность распознавания экстремистских материалов – 89%.

Помимо вышеперечисленных систем, в частности ресурсов «Помор» и «Отис», российские следователи активно используют и иные виды цифровых технологий со встроенным ИИ. Для распознавания лиц в следствии активно применяют систему «Видеоаналитика» [Computer Vision Video Content Analysis Машинное (компьютерное) зрение Системы видеоаналитики, www] – это программно-аппаратный комплекс, использующий технологии ИИ и компьютерного зрения для автоматического анализа видеопотоков в реальном времени. Данная система выполняет множество функций: распознавание объектов (лица, транспортные средства, поведение людей), детекция событий (нарушение периметра, кражи в магазинах, ДТП). Также «видеоаналитика» используется в системе «безопасный город», по последней имеющейся статистике, к 2024 году распознал более миллиона нарушений правил дорожного движения. Отметим, что данной системой пользуется сеть «Магнит», после ее внедрения количество краж в магазинах снизилась на 30%. Необходимо отметить, что кроме явных плюсов использование данной системы имеет и отрицательные последствия.

Органы внутренних дел также внедряют в свою работу систему для прогнозирования преступления. Система «Предикативная полиция» [«Особое мнение» нейросетей. Как с криминалом борются алгоритмами к ужасу правозащитников, www] — это технология на основе ИИ и анализа больших данных, которая прогнозирует места, время и вероятность совершения преступлений до их возникновения. Она помогает правоохранительным органам упреждающе распределять ресурсы (патрули, оперативные группы) для предотвращения преступности. Данная система в настоящее время только тестируется в некоторых районах Москвы и Санкт-Петербурга, но уже сейчас сообщаются о положительных тенденциях. После использовании данного ресурса наблюдается снижение уличной преступности на 15-20%, раскрытие серийных краж благодаря анализу геоданных.

На сегодняшний день органами МВД разрабатываются системы «Клон» и «Конъюнктура» [МВД РФ привлечет ИИ к поиску преступников, www] — это разрабатываемые МВД России платформы для прогнозной аналитики и управления правоохранительной

деятельностью на основе искусственного интеллекта. Данные ресурсы постепенно интегрируются в различные базы МВД, в систему «Безопасный город» и социальные сети. С помощью этой системы смогут прогнозировать возможности рецидива у освобожденных заключенных.

При расследовании преступлений, в частности, криминалистами используется система «Криминалист-ИИ» [Нейронное дело: как ИИ помогает в борьбе с преступностью, www]. Данная система обрабатывает отпечатки пальцев и ищет совпадения в базе данных всего за две секунды (вместо двух часов, когда это делают вручную). Также активно используется система «Фоторобот 5.5» [МВД: ИИ-система поиска серийных преступников и создания фотороботов, www], которая генерирует фото подозреваемого по описанию свидетелей с помощью GAN-сетей.

В настоящее время ИИ-технологии активно используют правоохранительные органы при расследовании преступлений. Приведем некоторые из них. В марте 2025 года МВД и ФСБ задержали 15 человек, причастных к созданию инфраструктуры связи, использовавшейся для телефонного мошенничества [Борьба с телефонным мошенничеством, www]. Министерство цифрового развития Республики Татарстан приступило к тестированию системы видеонаблюдения с искусственным интеллектом для выявления закладчиков наркотиков на улицах Казани, о чем стало известно 5 ноября 2024 года [Выявление в Казани закладчиков наркотиков с помощью ИИ-камер, www]. В 2020 г. в России был задержан подозреваемый в хищении бюджетных средств благодаря системе «Криминалист», которая анализирует данные из разных госсистем, а также открытых источников [Нейронное дело: как ИИ помогает в борьбе с преступностью, www].

Внедрение искусственного интеллекта (ИИ) в расследование преступлений вызывает активные дискуссии среди ученых, юристов и правозащитников. Приведем ключевые мнения экспертов из разных стран, отражающие как преимущества, так и риски этой технологии. Профессор Andrew Ng (Стэнфорд, США) высказывается положительно о внедрении ИИ в расследование преступлений: «ИИ может анализировать тысячи часов видеозаписей за минуты, находить связи между преступлениями и даже предсказывать зоны повышенной криминальной активности. Это революция для полицейской работы» [Выступление на конференции AI in Law Enforcement (2023): Stanford HAI – AI in Policing, www]. Также в поддержку использования ИИ высказался Доктор Marcus Peter Francis du Sautoy (Оксфорд, Великобритания), подметив, что «машинное обучение помогает выявлять паттерны в финансовых преступлениях, которые человек просто не заметит. Например, отмывание денег через криптовалюты» [Isaacson, 2022]. В том числе ряд ученых высказываются негативно на тему внедрения ИИ в расследование преступлений. Например, Профессор Joy Buolamwini (MIT, США) считает, что «ИИ-алгоритмы, обученные на предвзятых данных, усиливают расовую дискриминацию. Например, системы распознавания лиц чаще ошибаются с темнокожими людьми». В качестве факта он приводит исследование MIT Media Lab (2023) показало, что ошибки распознавания у афроамериканцев — до 34% против 1% у белых [Исследование по bias в распознавании лиц (MIT Media Lab), www]. Российский ученый, д.ю.н., профессор, советник МВД РФ, Овчинский В.С. также с настороженностью высказывается относительно данного вопрос – «Сегодня с технологией ИИ много проблем: она ненадежна, часто очень хрупка в том смысле, что системы ИИ могут хорошо работать в некоторых контекстах, а затем часто могут довольно серьезно выйти из строя в других» [Владимир Овчинский: Мощь искусственного интеллекта, www].

Существует множество высказываний ученых со всего мира относительно использовании ИИ-технологий в расследовании преступлений. Одна половина ученых считает внедрение

подобных систем спасением, другая же группа ученых высказывается против активного использования ИИ-технологий, ссылаясь на то, что еще нет достаточного регулирования применения подобных ресурсов. Полагаем, что мнения обеих групп ученых имеет право на существования. В использовании цифровых технологий, в которых встроен ИИ, есть как положительные, так и отрицательные стороны. Нам представляется, что внедрение искусственного интеллекта в работу правоохранительных органов дает значительные преимущества, ускоряя раскрываемость преступлений и повышая точность анализа данных, например:

1. ИИ анализирует тысячи часов видеозаписей, миллионы транзакций, переписки в соцсетях за минуты, что человеку не под силу.

2. Распознавание лиц, голоса, отпечатков пальцев, анализ метаданных, на примере деанонимизации в Darknet – там, где человеческий мозг бессилен, ИИ находит закономерности.

3. Алгоритмы предсказывают «горячие точки» преступности на основе исторических данных.

4. ИИ находит скрытые связи между преступниками, анализируя финансовые потоки (отмывание денег, мошенничество) и цепочки сообщений.

5. ИИ не подвержен усталости, эмоциям или предвзятости (если алгоритм правильно обучен).

Хотя искусственный интеллект значительно улучшает работу правоохранительных органов, его применение связано с серьезными рисками и недостатками, а поэтому необходимо выделить ключевые, важные, на наш взгляд, нюансы:

1. Алгоритмы могут ошибаться из-за некачественных данных или ограниченного обучения. Например: В США система Facial Recognition ошибочно идентифицировала невиновных (случай с Робертом Уильямсом в Детройте) [В США зафиксировано первое ошибочное задержание из-за технологии распознавания лиц, www].

2. ИИ обучается на исторических данных, которые могут содержать дискриминационные паттерны. Например, Система COMPAS (США) чаще рекомендовала арест для темнокожих подозреваемых [Судебная система США годами использовала программу-расиста, www].

3. Массовый сбор данных (камеры, биометрия, анализ переписок) создает риски, такие как утечки персональных данных и злоупотребление со стороны властей.

4. Проблемы с легитимностью и ответственностью. Можно ли доверять ИИ-доказательствам? Кто отвечает за ошибку? Разработчик, полиция или государство?

5. Зависимость от технологий и «ленивые следователи». Снижение критического мышления: сотрудники могут слепо доверять ИИ, упуская альтернативные версии;

6. Уязвимость к кибератакам. Взлом ИИ-систем может привести к фальсификации улик (например, deepfake-видео) или манипуляции данными (подмена результатов распознавания);

7. Высокая стоимость и неравный доступ. Внедрение ИИ требует больших затрат – не все регионы/страны могут позволить себе передовые системы. Например, в России «умные» камеры есть в Москве, но отсутствуют в малых городах.

Следует констатировать факт, что искусственный интеллект стал неотъемлемой частью современной криминалистики, предлагая революционные возможности, но одновременно создавая новые вызовы для общества. Главный парадокс заключается в том, что чем совершеннее технологии, тем острее встают такие вопросы, как где граница между помощью следователю и подменой человеческого суждения? Кто контролирует тех, кто контролирует алгоритмы?

Чтобы активно и безопасно внедрять ИИ-технологии в расследование реальных дел, на наш

взгляд, необходимо следующее:

1. Подготовка квалифицированных специалистов для работы с современными системами. В России для борьбы с киберпреступностью было учреждено Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий. Но на данный момент существует острая нехватка кадров не только в этом отделе, но и в целом в системе МВД РФ [В МВД оценили дефицит сотрудников в 172 тыс. человек, www]. В настоящее время большинство вузов в России по направлению подготовки «Юриспруденция» выпускают специалистов с общими познаниями в данной отрасли, существует нехватка узконаправленных специалистов. Для решения проблемы необходимо, на наш взгляд, открыть дополнительные кафедры, специальность, на которых будут обучать специалистов расследованию киберпреступлений и применению для этой цели ИИ-технологий. Ввести дополнительные курсы в специализированных вузах по борьбе с киберпреступностью либо уделить особое внимание данной теме в рамках практических занятий по дисциплине «Криминалистика».

2. Правовое регулирование использования ИИ-технологий в расследовании киберпреступлений. В настоящее время в России нет четких законов, определяющих рамки использования цифровых технологий со встроенным искусственным интеллектом. К примеру, 2 февраля 2025 в Европейском Союзе вступил в силу Акт об искусственном интеллекте (EU AI Act), устанавливающий ограничения на использование технологий ИИ.

3. Установление прозрачности использования ИИ-технологий. Алгоритмы должны быть объяснимыми, а не «черными ящиками».

4. Соблюдение баланса. Технологии должны дополнять, а не заменять профессиональное мнение следователей.

Заключение

Таким образом, технологии со встроенным искусственным интеллектом – это как мощный микроскоп в руках криминалиста. Сам по себе он не хорош и не плох – все зависит от того, кто, как и зачем его использует. Будущее расследований – не в слепом доверии алгоритмам, а в их разумной интеграции при сохранении человеческого контроля.

Библиография

1. Борьба с телефонным мошенничеством. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%80%D1%8C%D0%B1%D0%B0_%D1%81_%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D1%8B%D0%BC_%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE%D0%BC (дата обращения: 09.04.2025).
2. В МВД оценили дефицит сотрудников в 172 тыс. человек. URL: https://expert.ru/news/v-mvd-otsenili-defitsit-sotrudnikov-v-172-tys-chelovek/ (дата обращения: 09.04.2025).
3. В США зафиксировано первое ошибочное задержание из-за технологии распознавания лиц. URL: https://www.kommersant.ru/doc/4391519 (дата обращения: 09.04.2025).
4. Владимир Овчинский: Мощь искусственного интеллекта. URL: https://izborsk-club.ru/23996 (дата обращения: 09.04.2025).
5. Выступление на конференции AI in Law Enforcement (2023): Stanford HAI – AI in Policing. URL: https://hai.stanford.edu/news/how-ai-changing-law-enforcement (дата обращения: 09.04.2025).
6. Выявление в Казани закладчиков наркотиков с помощью ИИ-камер. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%

B5 (дата обращения: 09.04.2025).
7. ЕСИА. URL: https://info.gosuslugi.ru/articles/%D0%95%D0%A1%D0%98%D0%90/ (дата обращения: 09.04.2025).
8. Исследование по bias в распознавании лиц (MIT Media Lab). URL: http://gendershades.org/ (дата обращения: 09.04.2025).
9. МВД РФ привлечет ИИ к поиску преступников. URL: https://itspeaker.ru/news/mvd-rf-privlechet-ii-k-poisku-prestupnikov/ (дата обращения: 09.04.2025).
10. МВД: ИИ-система поиска серийных преступников и создания фотороботов. URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%9C%D0%92%D0%94:_%D0%98%D0%98-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BF%D0%BE%D0%B8%D1%81%D0%BA%D0%B0_%D1%81%D0%B5%D1%80%D0%B8%D0%B9%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2_%D0%B8_%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D1%8F_%D1%84%D0%BE%D1%82%D0%BE%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%BE%D0%B2 (дата обращения: 09.04.2025).
11. Нейронное дело: как ИИ помогает в борьбе с преступностью. URL: https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu (дата обращения: 09.04.2025).
12. «Особое мнение» нейросетей. Как с криминалом борются алгоритмами к ужасу правозащитников. URL: https://tass.ru/obschestvo/5941548 (дата обращения: 09.04.2025).
13. Открытая NLP-модель для классификации ESG-рисков. URL: https://developers.sber.ru/portal/products/esgify (дата обращения: 09.04.2025).
14. Подстава века или таинственная история взлома Ситибанка. URL: https://habr.com/ru/companies/macloud/articles/552866 (дата обращения: 14.04.2025).
15. Ростелеком усилил киберзащиту технологических процессов. URL: https://www.company.rt.ru/press/news/d472870/ (дата обращения: 09.04.2025).
16. Статистика киберпреступности в российских регионах: данные МВД за 2024 год». URL: https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/#:~:text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D0%B2%202024%20%D0%B3%D0%BE%D0%B4%D1%83%20%D0%B2,%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D1%8E%D1%82%20%D0%B4%D0%BE%D0%BF%D0%BE%D0%BB%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%B2%D0%BE%D0%B7%D0%BC%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D0%B4%D0%BB%D1%8F%20%D0%B7%D0%BB%D0%BE%D1%83%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2 (дата обращения: 09.04.2025).
17. Судебная система США годами использовала программу-расиста. URL: https://mir24.tv/news/16261623/sudebnaya-sistema-ssha-godami-ispolzovala-programmu-rasista (дата обращения: 09.04.2025).
18. Computer Vision Video Content Analysis Машинное (компьютерное) зрение Системы видеоаналитики. URL: https://www.tadviser.ru/index.php/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8 (дата обращения: 09.04.2025).
19. Internet Crime Complaint Center (IC3). URL: https://www.ic3.gov/ (дата обращения: 09.04.2025).
20. Isaacson W. The Code Breaker. 2022. P. 560. URL: https://www.labirint.ru/books/965920.
21. Kaspersky Machine Learning for Anomaly Detection. URL: https://mlad.kaspersky.ru/ (дата обращения: 09.04.2025).

Using digital technologies with artificial intelligence in the fight against cybercrime in Russia and abroad

Arkadii R. Sirakanyan

PhD in Law,
Deputy Director of the Institute of State and Law
of Surgut State University,
628412, 1 Lenina str., Surgut, Russian Federation;
e-mail: Sirakanyan_ar@surgu.ru

Abstract

The article research modern methods of using digital technologies and artificial intelligence to counter cybercrime in Russia and abroad. The key tools used by law enforcement agencies, including big data analysis, pattern recognition, and predictive analytics systems, are reviewed. The advantages of artificial intelligence are analyzed, including the speed of information processing and automation of routine tasks, as well as problems related to algorithm errors, privacy issues and the need for legal regulation. The article presents the opinions of scientists regarding the use of digital technologies with embedded intelligence and provides the author's opinion on this issue. Examples of real-world cases where technology has helped solve crimes are given, and prospects for the development of AI tools in the context of national cybersecurity are discussed. The article is intended for specialists in the field of digital forensics, law enforcement agencies and anyone interested in the technological aspects of combating cybercrime.

For citation

Sirakanyan A.R. (2025) Ispol'zovanie tsifrovykh tekhnologii s iskusstvennym intellektom v bor'be s kiberprestupnost'yu v Rossii i zarubezhom [Using digital technologies with artificial intelligence in the fight against cybercrime in Russia and abroad]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (2A), pp. 506-515.

Keywords

Artificial intelligence, forensic *science*, criminalistics, big data analysis, machine learning, Russian AI technologies.

References

1. *Bor'ba s telefonnym moshennichestvom* [Fight against telephone fraud] (2025). Tadviser. Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%80%D1%8C%D0%B1%D0%B0_%D1%81_%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D1%8B%D0%BC_%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE%D0%BC [Accessed 09 April 2025].
2. V MVD otsenili defitsit sotrudnikov v 172 tys. chelovek [Ministry of Internal Affairs estimated staff shortage at 172 thousand people] (2025). *Expert*. Available at: https://expert.ru/news/v-mvd-otsenili-defitsit-sotrudnikov-v-172-tys-chelovek/ [Accessed 09 April 2025].
3. V SShA zafiksirovano pervoe oshibochnoe zaderzhanie iz-za tekhnologii raspoznavaniia lits [First erroneous arrest due to facial recognition technology recorded in the USA] (2025). *Kommersant*. Available at: https://www.kommersant.ru/doc/4391519 [Accessed 09 April 2025].
4. Vladimir Ovchinskii: Moshch iskusstvennogo intellekta [Vladimir Ovchinsky: The Power of Artificial Intelligence] (2025). *Izborsk Club*. Available at: https://izborsk-club.ru/23996 [Accessed 09 April 2025].
5. *Vystuplenie na konferentsii AI in Law Enforcement (2023): Stanford HAI – AI in Policing* [Speech at the conference AI in Law Enforcement (2023): Stanford HAI – AI in Policing] (2023). Stanford HAI. Available at: https://hai.stanford.edu/news/how-ai-changing-law-enforcement [Accessed 09 April 2025].
6. *Vyiavlenie v Kazani zakladchikov narkotikov s pomoshch'iu II-kamer* [Detection of drug dealers in Kazan using AI cameras] (2025). Tadviser. Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5 [Accessed 09 April 2025].
7. *ESIA* [Unified Identification and Authentication System] (2025). Gosuslugi. Available at: https://info.gosuslugi.ru/articles/%D0%95%D0%A1%D0%98%D0%90/ [Accessed 09 April 2025].
8. Issledovanie po bias v raspoznavanii lits (MIT Media Lab) [Study on bias in facial recognition (MIT Media Lab)] (2025). *MIT Media Lab*. Available at: http://gendershades.org/ [Accessed 09 April 2025].

9. MVD RF privlechet II k poiskam prestupnikov [Ministry of Internal Affairs of Russia will involve AI in searching for criminals] (2025). *ITSpeaker*. Available at: https://itspeaker.ru/news/mvd-rf-privlechet-ii-k-poisku-prestupnikov/ [Accessed 09 April 2025].
10. MVD: II-sistema poiska seriinykh prestupnikov i sozdaniia fotorobotov [Ministry of Internal Affairs: AI system for searching serial criminals and creating facial composites] (2025). *Tadviser*. Available at: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%9C%D0%92%D0%94:_%D0%98%D0%98-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BF%D0%BE%D0%B8%D1%81%D0%BA%D0%B0_%D1%81%D0%B5%D1%80%D0%B8%D0%B9%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2_%D0%B8_%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D1%8F_%D1%84%D0%BE%D1%82%D0%BE%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%BE%D0%B2 [Accessed 09 April 2025].
11. Neironnoe delo: kak II pomogaet v bor'be s prestupnost'iu [Neural case: how AI helps in the fight against crime] (2025). *Izvestia*. Available at: https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu [Accessed 09 April 2025].
12. «Osoboe mnenie» neirosetei. Kak s kriminalom boriutsia algoritmami k uzhasu pravozashchitnikov ["Minority Report" of neural networks. How algorithms fight crime to the horror of human rights activists] (2025). *TASS*. Available at: https://tass.ru/obschestvo/5941548 [Accessed 09 April 2025].
13. Otkrytaia NLP-model' dlia klassifikatsii ESG-riskov [Open NLP model for ESG risk classification] (2025). *SberDev*. Available at: https://developers.sber.ru/portal/products/esgify [Accessed 09 April 2025].
14. Podstava veka ili tainstvennaia istoriia vzloma Sitibanka [The setup of the century or the mysterious story of Citibank's hack] (2025). *Habr*. Available at: https://habr.com/ru/companies/macloud/articles/552866 [Accessed 14 April 2025].
15. Rostelekom usilil kiberzashchitu tekhnologicheskikh protsessov [Rostelecom strengthened cybersecurity of technological processes] (2025). *Rostelecom*. Available at: https://www.company.rt.ru/press/news/d472870/ [Accessed 09 April 2025].
16. Statistika kiberprestupnosti v rossiiskikh regionakh: dannye MVD za 2024 god [Cybercrime statistics in Russian regions: Ministry of Internal Affairs data for 2024] (2024). *EC-RS*. Available at: https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/#:~:text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D0%B2%202024%20%D0%B3%D0%BE%D0%B4%D1%83%20%D0%B2,%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D1%8E%D1%82%20%D0%B4%D0%BE%D0%BF%D0%BE%D0%BB%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%B2%D0%BE%D0%B7%D0%BC%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%B8%20%D0%B4%D0%BB%D1%8F%20%D0%B7%D0%BB%D0%BE%D1%83%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2 [Accessed 09 April 2025].
17. Sudebnaia sistema SShA godami ispol'zovala programmu-rasista [US judicial system used a racist program for years] (2025). *Mir24*. Available at: https://mir24.tv/news/16261623/sudebnaya-sistema-ssha-godami-ispolzovala-programmu-rasista [Accessed 09 April 2025].
18. Computer Vision Video Content Analysis Mashinnoe (komp'iuternoe) zrenie Sistemy videoanalitiki [Computer Vision Video Content Analysis Machine (computer) vision Video analytics systems] (2025). *Tadviser*. Available at: https://www.tadviser.ru/index.php/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8 [Accessed 09 April 2025].
19. Internet Crime Complaint Center (IC3) (2025). *FBI*. Available at: https://www.ic3.gov/ [Accessed 09 April 2025].
20. Isaacson W. (2022). *The Code Breaker*. Available at: https://www.labirint.ru/books/965920 [Accessed 09 April 2025].
21. Kaspersky Machine Learning for Anomaly Detection (2025). *Kaspersky*. Available at: https://mlad.kaspersky.ru/ [Accessed 09 April 2025].