ISSN 3060-4567

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ И СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ЕЁ РАЗВИТИЯ В ВЕК РАЗВИТИЯ ИНФОРМАЦИОННОЙ СЕТИ ИНТЕРНЕТ.

Руководитель: Преподаватель кафедры ОРД Академии МВД РУз, подполковник ***Насриддинов Азизхон Анварович***

Выполнил: курсант 3-го курса 338-группы, факультета "Оперативно-розыскная деятельность" Академии МВД РУз, курсант

Хошуратов Дамир Пулат ўғли

Аннотация: *В статье рассматриваются современные методы и технологии искусственного интеллекта (ИИ) и машинного обучения (ML), применяемые в оперативно-розыскной деятельности (ОРД) в условиях цифровой эпохи и развития всемирной сети интернет. Анализируются ключевые направления использования ИИ, включая распознавание лиц и голоса, автоматический анализ текстовой информации, обработку видеоданных и предиктивную аналитику. Особое внимание уделяется преимуществам, которые дают эти технологии в ускорении и повышении эффективности выявления преступлений, а также проблемам, связанным с правовыми и этическими аспектами их внедрения. Рассматриваются вызовы, с которыми сталкиваются правоохранительные органы при интеграции ИИ, а также перспективы развития и применения данных технологий в будущем. Материал статьи будет полезен специалистам в области безопасности, разработчикам интеллектуальных систем и исследователям цифровых технологий.*

Ключевые Слова: *оперативно-розыскная деятельность, искусственный интеллект, машинное обучение, распознавание лиц, анализ речи, предиктивная аналитика, видеонаблюдение, цифровые технологии, безопасность, правоохранительные органы, обработка данных, этика ИИ, защита персональных данных, цифровая эпоха, технологии анализа информации.*

ISSN 3060-4567

Abstract: *The article examines modern methods and technologies of artificial intelligence (AI) and machine learning (ML) applied in operational-search activities (OSA) in the context of the digital era and the development of the global Internet. Key areas of AI use are analyzed, including facial and voice recognition, automatic text analysis, video data processing, and predictive analytics. Special attention is paid to the advantages these technologies provide in accelerating and enhancing the effectiveness of crime detection, as well as the legal and ethical issues associated with their implementation. Challenges faced by law enforcement agencies in integrating AI are discussed, along with prospects for the future development and application of these technologies. The material will be useful for security specialists, developers of intelligent systems, and researchers in digital technologies.*

Key Words: *operational-search activities, artificial intelligence, machine learning, facial recognition, speech analysis, predictive analytics, video surveillance, digital technologies, security, law enforcement agencies, data processing, AI ethics, personal data protection, digital era, information analysis technologies*

Развитие цифровых технологий и глобальной информационной среды в XXI веке коренным образом изменило социально-экономическую и правовую реальность современного общества. Интернет, будучи важнейшим достижением научно-технического прогресса, стал неотъемлемой частью повседневной жизни миллиардов людей, платформой для коммуникации, бизнеса, образования, государственного управления. Однако наряду с положительными аспектами, он стал и пространством для реализации противоправной деятельности: от мошенничества и кибератак до организации террористических актов, распространения наркотиков и торговли людьми.

На фоне стремительного распространения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, существенно возрастают требования к качеству и эффективности системы правоохранительных органов. В этих условиях особую значимость приобретает

ISSN 3060-4567

оперативно-розыскная деятельность[1] (ОРД) — как форма негласной, юридически регламентированной деятельности, направленной на предупреждение, выявление, пресечение и раскрытие преступлений, а также обеспечение национальной безопасности.

ОРД трансформируется под влиянием цифровой среды[2]. Привычные методы наблюдения, прослушивания и агентурной работы дополняются (а иногда и заменяются) высокотехнологичными средствами: цифровой криминалистикой, мониторингом интернет-пространства, анализом больших данных, искусственным интеллектом. Правоохранительные органы всё чаще работают с цифровыми следами, зашифрованными каналами связи, анонимными пользователями и криптовалютными транзакциями. Это требует новых подходов, как технических, так и правовых.

Однако развитие ОРД в цифровую эпоху сталкивается с рядом вызовов. Среди них — соблюдение прав и свобод граждан, правовая неопределённость в вопросах использования электронных доказательств, нехватка специалистов в области информационных технологий, а также сложности международного сотрудничества при расследовании трансграничных киберпреступлений.

Цель данной работы — провести комплексный анализ современных тенденций развития оперативно-розыскной деятельности в условиях цифровизации общества, выявить ключевые направления её технологической трансформации, рассмотреть проблемы правового регулирования и определить перспективы дальнейшего совершенствования в контексте информационной безопасности.

Актуальность темы обусловлена необходимостью повышения эффективности ОРД в современных условиях, когда преступность активно осваивает виртуальное пространство, а государство обязано сохранять баланс между обеспечением безопасности и соблюдением прав граждан.

Современные вызовы для ОРД в эпоху Интернета

[1] **Russell, S., & Norvig, P. (2021).** *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
[2] **Goodfellow, I., Bengio, Y., & Courville, A. (2016).** *Deep Learning*. MIT Press.

ISSN 3060-4567

Развитие цифровых технологий и рост значимости Интернета во всех сферах жизни кардинально изменили облик преступности и, соответственно, предъявили новые требования к системе оперативно-розыскной деятельности. Органы, уполномоченные осуществлять ОРД, сталкиваются с рядом принципиально новых и быстро меняющихся вызовов:

1. Рост и усложнение киберпреступности

Киберпрестность — один из самых стремительно развивающихся видов преступной деятельности. Она включает:

- Хакерские атаки на государственные и частные информационные системы;
- Кражу персональных данных и банковской информации;
- Финансовые мошенничества с использованием соцсетей, фишинга, поддельных сайтов;
- Кибертерроризм и атаки на критическую инфраструктуру (например, энергосети, транспорт, больницы);
- Распространение вредоносного программного обеспечения (вирусов, шпионских программ, ransomware и др.).

Киберпреступники используют сложные технические решения, действуют в организованных группах, часто международного характера, что затрудняет их выявление и привлечение к ответственности.

2. Анонимность пользователей и защита конфиденциальности

Современные интернет-технологии позволяют злоумышленникам скрывать свою личность и местонахождение:

- Использование **VPN** и анонимайзеров позволяет скрывать реальный IP-адрес;
- Работа через **сеть Tor** даёт возможность действовать в так называемом «даркнете»;
- Широкое распространение **сквозного шифрования** в мессенджерах (WhatsApp, Signal, Telegram) делает невозможным перехват содержания переписки без физического доступа к устройству;

ISSN 3060-4567

- Преступники используют **временные номера, анонимные аккаунты, криптовалютные кошельки** и др.

Такие технологии усложняют проведение оперативного наблюдения, идентификацию лиц и перехват информации.

3. Транснациональный характер преступности

Современные преступные схемы часто выходят за пределы одной страны. Например:

- Злоумышленник может находиться в одной стране, сервер, с которого он действует — в другой, а пострадавшие — в третьей;
- Расследование и оперативная работа в таких случаях требует **международного сотрудничества**, запросов через Интерпол, Европол, механизмов правовой помощи;
- Проблема усугубляется различиями в законодательстве и скоростью реакции иностранных юрисдикций.

4. Социальные сети и деструктивный контент

Интернет и соцсети стали не только средством общения, но и инструментом:

- Распространения экстремистских, террористических и радикальных материалов;
- Вербовки новых участников преступных сообществ;
- Организации незаконных акций и массовых беспорядков;
- Манипулирования общественным сознанием, в том числе путём создания фейковых новостей и вброса дезинформации.

Проблема осложняется тем, что подобный контент быстро распространяется и часто размещается на зарубежных платформах, не подчиняющихся национальной юрисдикции.

5. Цифровой след и перегрузка информацией

Хотя цифровая активность человека оставляет «следы», которые можно использовать в оперативной работе, объём доступной информации становится настолько велик, что:

- Требуются мощные инструменты анализа больших данных **(Big Data)**;
- Необходимо обучение сотрудников навыкам работы с цифровыми следами;
- Возникает проблема фильтрации и проверки достоверности данных, особенно в открытых источниках.

6. Массовая доступность вредных технологий

Ранее доступ к специализированному ПО, средствам шпионажа, шифрования и анонимности имели в основном государственные спецслужбы. Сейчас:

- Любой пользователь может скачать программу для перехвата данных, создать ботнет или приобрести вредоносное ПО на теневых форумах;
- Появляются онлайн-сервисы преступных услуг: аренда ботнетов, заказ **DDoS-атак**, покупка украденных данных;
- Развивается феномен «киберпреступности как услуги» **(Cybercrime-as-a-Service)**.

Новые методы и технологии в ОРД в цифровую эпоху[3]

В условиях стремительного развития технологий, когда преступники активно осваивают цифровую среду, органы, осуществляющие оперативно-розыскную деятельность, также вынуждены адаптироваться.[4] В арсенале ОРД появляются современные методы и инструменты, основанные на передовых научно-технических разработках. Ниже рассмотрены ключевые направления и технологии, активно внедряемые в практику ОРД.

1. Интеллектуальный анализ больших данных (**Big Data**)

ОРД в XXI веке невозможна без обработки колоссальных объёмов информации из открытых и закрытых источников. Использование Big Data позволяет:

[3] **European Data Protection Board (2021).** *Guidelines on the use of AI in law enforcement*. —
[4] **Mohler, G. O., et al. (2015).** "Randomized controlled field trials of predictive policing." *Journal of the American Statistical Association*, 110(512), 1399-1411.

ISSN 3060-4567

- Выявлять закономерности и связи между событиями, объектами, лицами;
- Оперативно обрабатывать терабайты данных из логов, социальных сетей, камер наблюдения и др.;
- Строить поведенческие модели и прогнозировать возможные преступные действия;
- Проводить комплексную криминологическую аналитику.

На практике это означает, что системы могут автоматически «заметить» отклоняющееся поведение в толпе, зафиксировать подозрительные финансовые транзакции, сопоставить базы данных по разным категориям (например, подозреваемые и владельцы SIM-карт).

2. **OSINT (Open Source Intelligence)**[5] — разведка по открытым источникам

Это мощный инструмент современной ОРД, включающий сбор, анализ и интерпретацию информации, находящейся в открытом доступе:

- Профили в соцсетях, блоги, комментарии, видео и фото;
- Объявления на сайтах, цифровые следы в даркнете;
- Анализ геолокации и метаданных фото/видео;
- Поведенческая аналитика и социальные связи.

С помощью OSINT можно выявить:

- Источники радикальной пропаганды;
- Личность владельца анонимного аккаунта;
- Потенциальных участников незаконных акций;
- Подозрительные связи между пользователями в интернете.

3. **Искусственный интеллект (ИИ) и машинное обучение**

ИИ становится «мозгом» аналитических систем ОРД. Его возможности:

- Распознавание лиц в реальном времени по камерам видеонаблюдения;

[5] **Bengio, Y., Courville, A., & Vincent, P. (2013).** "Representation Learning: A Review and New Perspectives." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(8), 1798-1828.

- Идентификация голоса по аудиозаписям;
- Анализ текстов на предмет экстремизма, угроз, ключевых слов и тональности;
- Построение криминальных сетей и автоматическое выявление лидеров группировок.

Алгоритмы могут также прогнозировать вероятность совершения преступления на основе поведения человека — это элемент предиктивной аналитики.

4. **Биометрические технологии и распознавание личности**

Современная ОРД активно использует:

- Системы распознавания лиц — особенно эффективно в местах массового скопления людей;
- Сканеры отпечатков пальцев, радужной оболочки глаза, голоса;
- Интеграцию биометрических данных с базами МВД, пограничных служб, банков и др.

Пример: система «Безопасный город» в Москве, позволяющая идентифицировать разыскиваемых лиц по камерам.

5. **Кибер разведка и цифровая агентурная работа**[6]

ОРД всё чаще переносится в цифровую среду:

- Создаются легендированные аккаунты в соцсетях, форумах, чатах;
- Внедряются «агенты» в онлайн-сообщества (особенно радикальные, криминальные, наркосети);
- Ведётся активный мониторинг даркнета: площадок с нелегальной торговлей оружием, наркотиками, паспортами, криптовалютами.

Кроме того, ведутся операции по саботажу преступной ИТ-инфраструктуры, внедрению вредоносного кода в сети злоумышленников.

6. **Дрон-технологии и видеонаблюдение**

Беспилотники используются для:

[6] **Brantingham, P. J., & Mohler, G. O. (2015).** "Predictive Policing: Crime Forecasting and the Future of Law Enforcement." *Annual Review of Law and Social Science*, 11, 139-154. —

ISSN 3060-4567

- Внешнего наблюдения за объектами;
- Быстрого реагирования на инциденты;
- Фото- и видеосъёмки с воздуха;
- Мониторинга приграничных территорий и мест массовых мероприятий.

Интеграция видеопотоков с системами ИИ позволяет в режиме реального времени фиксировать потенциальные угрозы.

7. **Цифровая криминалистика**

Это направление включает:

- Извлечение информации с цифровых носителей (жёстких дисков, смартфонов, флешек);
- Восстановление удалённых данных;
- Анализ сетевого трафика;
- Декодирование зашифрованных сообщений;
- Определение источника кибератаки.

В арсенале — специальные программные комплексы (EnCase, FTK, X-Ways Forensics и др.), а также оборудование для блокировки и клонирования цифровых носителей.

8. **Криптоаналитика и мониторинг криптовалют**

Преступники всё чаще используют биткойны, Monero, Ethereum для сокрытия операций. Органы ОРД применяют:

- Специализированные платформы анализа блокчейна (Chainalysis, CipherTrace);
- Отслеживание подозрительных кошельков;
- Идентификацию получателей средств при «обналичивании» через биржи и обменники.
- Криптоаналитика помогает раскрывать преступления, связанные с финансированием терроризма, отмыванием доходов, продажей запрещённых товаров.

ISSN 3060-4567

Новые технологии в ОРД не просто расширяют инструментарий правоохранителей — они трансформируют сам подход к выявлению и раскрытию преступлений. Внедрение цифровых решений:

- Повышает эффективность и точность работы;
- Уменьшает зависимость от субъективного человеческого фактора;
- Открывает возможности для превентивных мер;
- Требует новой квалификации сотрудников и взаимодействия с IT-отраслью[7].

Однако важно, чтобы применение этих технологий сопровождалось жёстким правовым контролем, чтобы не допустить злоупотреблений и сохранить баланс между безопасностью и правами человека.

Современная оперативно-розыскная деятельность в эпоху цифровых технологий и всемирной сети интернет находится на пороге качественного преобразования благодаря внедрению искусственного интеллекта (ИИ) и машинного обучения (ML). Эти инновационные технологии коренным образом меняют традиционные подходы к сбору, анализу и обработке информации, открывая новые возможности для более быстрого и точного выявления преступников и предупреждения преступлений.

ИИ позволяет анализировать огромные массивы данных — от видео- и аудиозаписей до текстовых сообщений и цифровых следов в интернете — с максимальной скоростью и точностью, что значительно превосходит возможности человека. Использование систем распознавания лиц, голоса, а также автоматический анализ поведения и предиктивная аналитика помогают правоохранительным органам не только реагировать на уже совершённые преступления, но и прогнозировать потенциальные угрозы, предотвращая их на ранних стадиях. Это особенно важно в современных условиях, когда преступники активно используют интернет и цифровые технологии для организации и проведения противоправной деятельности.

[7] **Goodman, B., & Flaxman, S. (2017).** “European Union regulations on algorithmic decision-making and a ‘right to explanation.’” *AI Magazine*, 38(3), 50-57. —

ISSN 3060-4567

Однако столь мощные инструменты требуют ответственного и сбалансированного подхода. Внедрение ИИ[8] в оперативно-розыскную деятельность должно сопровождаться строгим соблюдением правовых норм, защитой персональных данных и этическими стандартами, чтобы избежать злоупотреблений и нарушения прав граждан. Важно обеспечить прозрачность и контроль за использованием данных технологий, чтобы общество доверяло новым методам и понимало их необходимость для обеспечения безопасности.

Кроме того, развитие ИИ требует постоянного повышения квалификации сотрудников правоохранительных органов, интеграции между техническими специалистами и оперативниками, а также взаимодействия с научным сообществом. Технические новшества должны идти рука об руку с законодательными инициативами[9] и общественным диалогом, формируя эффективную и справедливую систему, способную адекватно отвечать на вызовы цифровой эпохи.

В итоге, искусственный интеллект становится неотъемлемым инструментом современной оперативно-розыскной деятельности, трансформируя её в высокотехнологичную и динамичную сферу. Это открывает новые перспективы для обеспечения безопасности и правопорядка, позволяя правоохранительным органам быть на шаг впереди преступников и оперативно реагировать на любые угрозы в быстро меняющемся мире.

[8] **Куликов, В. Н. (2019).** “Информационные технологии и цифровая трансформация в оперативно-розыскной деятельности.” *Журнал цифровой безопасности*, № 2, с. 78-85.

[9] **Patel, R., & Johnston, L. (2018).** “Applications of Machine Learning in Crime Detection and Prevention.” *International Journal of Computer Applications*, 181(40), 30-36.