Қазақстан Республикасы ІІМ Басқару академиясы
Академия управления МВД Республики Казахстан

ҚЫЛМЫСТЫЛЫҚҚА ҚАРСЫ ІС-ҚИМЫЛДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ

Халықаралық ғылыми-практикалық конференциясының

МАТЕРИАЛДАР ЖИНАҒЫ

2026 жылғы 18 қыркүйек

СБОРНИК МАТЕРИАЛОВ

Международной научно-практической конференции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ

18 сентября 2026 года



Астана • 2026

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект»

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
БАСҚАРУ АКАДЕМИЯСЫ

АКАДЕМИЯ УПРАВЛЕНИЯ
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

«ҚЫЛМЫСТЫЛЫҚҚА ҚАРСЫ ІС-ҚИМЫЛДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ»

Халықаралық ғылыми-практикалық конференциясының

МАТЕРИАЛДАР ЖИНАҒЫ

(2026 жылғы 18 қыркүйек)

СБОРНИК МАТЕРИАЛОВ

Международной научно-практической конференции

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ
В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ»

(18 сентября 2026 года)

Астана қаласы

УДК 343.9:004.8
ББК 67.51
Қ83

Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясының
Ғылыми кеңесінің шешімі бойынша басып шығарылады.

Жалпы редакциясын басқарған: **ДИЛЬБАРХАНОВА Ж.Р.**
Редакция алқасы: **Алимова Э.А., Кан А.Г., Жанхан Н., Лакбаев К.С., Мусин А.Б.**

Қ83 «Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» атты халықаралық ғылыми-практикалық конференция материалдары (2026 жылғы 18 қыркүйек). – Астана: Қазақстан Республикасы ІІМ Басқару академиясы, 2026. – _298_ б.

ISBN 978-601-360-299-8

Жинаққа «Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясы аясында ұсынылған ғылыми материалдар енгізілді. Конференция материалдары ғалымдарға, зерттеушілерге, білім алушыларға, құқық қорғау органдарының қызметкерлеріне, сондай-ақ жасанды интеллект пен цифрлық технологияларды қылмыстылыққа қарсы іс-қимыл саласында қолдану мәселелеріне қызығушылық танытатын мамандарға арналған.

В сборник включены научные материалы, представленные в рамках Международной научно-практической конференции «Искусственный интеллект в противодействии преступности». Материалы конференции предназначены для ученых, исследователей, обучающихся, сотрудников правоохранительных органов, а также специалистов, интересующихся вопросами применения искусственного интеллекта и цифровых технологий в сфере противодействия преступности.

Жинақтағы материалдар автордың редакциясымен берілді. Жинаққа енгізілген материалдардың мазмұны, келтірілген деректердің дұрыстығы және авторлық ұстанымдар үшін авторлар жауапты.

Материалы сборника представлены в авторской редакции. Ответственность за содержание включенных в сборник материалов, достоверность приведенных сведений и изложенную авторскую позицию несут авторы.

УДК 343.9:004.8
ББК 67.51
Қ83

ISBN 978-601-360-299-8

© Қазақстан Республикасы ІІМ Басқару академиясы, 2026

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясының БАҒДАРЛАМАСЫ

Өткізу күні мен уақыты	2026 жылғы 18 қыркүйек, сағат 09.30, Астана уақыты бойынша
Өткізу орны	Қазақстан Республикасы, Астана қ., Қазақстан Республикасы ІІМ Басқару академиясы, Мәңгілік Ел даңғылы, 55Б
Өткізу форматы	Аралас формат – **QOSYL** коммуникациялық платформасын пайдалана отырып, офлайн / онлайн / сырттай
Модератор	Қанат Сәметұлы Лақбаев Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының аға ғылыми қызметкері, заң ғылымдарының докторы, профессор

09:30 – 10:00	- Конференция қатысушыларын тіркеу - Онлайн жүйеге қосылу - Техникалық жағдайларды тексеру
10:00 – 10:20	- Конференцияның ашылуы - Кіріспе сөз
10:20 – 12:00	- Сессия жұмысы – баяндамалармен сөз сөйлеу
12:00 – 12:30	- Пікірталас, талқылау - Конференция қорытындыларын шығару - Естелік фотосуретке түсу

Кіріспе сөз: 5 минут
Сөйлеу регламенті: 7-10 минут
Іс-шараға қатысушылар offline / online:
ТМД елдерінің өкілдері, Қазақстан Республикасы ІІМ, Қазақстан Республикасы ІІМ Басқару академиясының өкілдері, жоғары оқу орындары және IT-қоғамдастықтар

КОНФЕРЕНЦИЯНЫҢ АШЫЛУЫ		
10:00 – 10:05	offline	**Кіріспе сөз** **Жанат Рахымжанқызы Дильбарханова** Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясының бастығы, заң ғылымдарының докторы, профессор, полиция полковнигі
10:05 – 10:10	offline	**Кіріспе сөз** **Эльвира Әбдіқапбарқызы Алимова** Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясы бастығының орынбасары, философия докторы (PhD), қауымдастырылған профессор (доцент), полиция полковнигі
10:10 – 10:15	offline	**Кіріспе сөз** **Әлібек Сайлауұлы Оразалы** Қазақстан Республикасы ІІМ Киберқылмысқа қарсы іс-қимыл департаменті бастығының орынбасары, техника ғылымдарының кандидаты, полиция полковнигі

СЕССИЯ ЖҰМЫСЫ // Баяндамалар		
УАҚЫТЫ	**ҚАТЫСУ ФОРМАТЫ**	**БАЯНДАМА ТАҚЫРЫБЫ ЖӘНЕ БАЯНДАМАШЫЛАР**
10:20 – 10:30	offline – баяндамамен сөз сөйлеу	**«Қазіргі кезеңдегі қылмыстылыққа қарсы іс-қимыл: ЖІҚ теориясының рөлі»** **Серік Жақыпбекұлы Ғалие**в Заң ғылымдарының кандидаты, доцент, Қазақстан Республикасы ІІМ-нің еңбек сіңірген қызметкері
10:30 – 10:40	offline – баяндамамен сөз сөйлеу	**«Киберқылмыстылыққа қарсы күрестегі халықаралық өзара іс-қимылдың кейбір аспектілері»** **Бейбіт Қайратұлы Біржанов** Қазақстан Республикасы ІІМ Киберқылмысқа қарсы іс-қимыл департаментінің 5-басқармасының бастығы, полиция полковнигі
10:40 – 10:45	offline – баяндамамен сөз сөйлеу	**«Цифрлық платформалардағы есірткіге байланысты контентті мониторингтеу және талдау үшін жасанды интеллектіні пайдалану»** **Василий Владимирович Гриценко** Қазақстан Республикасы ІІМ Есірткі қылмысына қарсы іс-қимыл комитетінің 6-басқармасының бастығы, полиция полковнигі
10:45 – 10:55	offline – баяндамамен сөз сөйлеу	TSARKA қызметі және ғылыми-техникалық әзірлемелер Руслан Амрканович Тургульдинов «Кибершабуылдарды талдау және тергеу орталығы» заңды тұлғалар бірлестігі президентінің орынбасары
10:55 – 11:05	offline – баяндамамен сөз сөйлеу	**«Жедел-іздестіру психологиясы: проблемалары мен келешегі»** **Қанат Сәметұлы Лақбаев** Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының аға ғылыми қызметкері, заң ғылымдарының докторы, профессор
11:05 – 11:15	offline – баяндамамен сөз сөйлеу	**«Құқыққа қайшы қызметті анықтау, талдау және жолын кесу мақсатында бұқаралық ақпарат құралдарын мониторингтеу үшін жасанды интеллект технологияларын пайдалану»** **Дәурен Қуанышұлы Рсалиев** «Seven Hills of Kazakhstan» ЖШС өкілі
11:15 – 11:25	offline – баяндамамен сөз сөйлеу	**«Жедел-іздестіру қызметінің өзекті проблемалары: цифрландыру жағдайындағы теория, заңнама және құқық қолдану практикасы»** **Мейрам Азаматұлы Жұмабаев** «Esbol Qory» қоғамдық қорының жобалар менеджері,

		құқықтанушы
11:25 – 11:35	online – баяндамамен сөз сөйлеу	**«Цифрландыру және жасанды интеллект жүйелерін енгізу жағдайында жастар экстремизміне жедел-іздестіру арқылы қарсы іс-қимылды трансформациялау»** **«Трансформация оперативно-розыскного противодействия молодежному экстремизму в условиях цифровизации и внедрения систем искусственного интеллекта»** (Тәжікстан Республикасы мысалында) **Абдуллозода Неъматулло Рахматулло** Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі кафедрасының бастығы, заң ғылымдарының кандидаты
11:35 – 11:40	offline – баяндамамен сөз сөйлеу	**«Реактивті модельден проактивті модельге: Қазақстан Республикасы ІІМ жедел-іздестіру қызметіндегі жасанды интеллект»** **Айдар Булатович Мусин** Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының аға ғылыми қызметкері, философия докторы (PhD), полиция майоры
11:40 – 11:50	online – баяндамамен сөз сөйлеу	**«Жедел-іздестіру қызметінде жасанды интеллектіні пайдалану проблемалары»** **Юлия Радиковна Хамзяев**а Ресей ІІМ Қазан заң институтының жедел-іздестіру қызметі кафедрасының бастығы, заң ғылымдарының кандидаты, полиция подполковнигі
11:50 – 12:00	online – баяндамамен сөз сөйлеу	**«Электрондық қылмыстық іс: құру архитектурасы және Ресейдің құқықтық жүйесіне бейімдеу»** **Моругина Надежда Анатольевна** Ресей ІІМ Воронеж институтының қылмыстық процесс кафедрасының доценті, заң ғылымдарының кандидаты, доцент, полиция полковнигі
12:00 – 12:30	Пікірталас, талқылау Конференция қорытындыларын шығару Естелік фотосуретке түсу	

ПРОГРАММА
международной научно-практической конференции
«Искусственный интеллект в противодействии преступности»

Дата и время проведения	18 сентября 2026 г. 09.30 ч. по Астанинскому времени
Место проведения	Республика Казахстан, г. Астана, Академия управления МВД Республики Казахстан, проспект Мәңгілік Ел, 55Б.
Формат проведения	Комбинированный формат – offline / online с использованием коммуникационной платформы **QOSYL** / заочная
Модератор	Канат Саметович Лакбаев Старший научный сотрудник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор юридических наук, профессор

09:30 – 10:00	- Регистрация участников конференции - Подключение к онлайн системе - Проверка технических условий
10:00 – 10:20	- Открытие конференции - Приветственное слово
10:20 – 12:00	- Работа сессии – выступления с докладами
12:00 – 12:30	- Дискуссия, обсуждение - Подведение итогов конференции - Памятное фотографирование

Приветственное слово: 5 минут
Регламент выступлений: 7-10 минут
Участники мероприятия offline / online:
Зарубежные представители СНГ, представители МВД Республики Казахстан, Академии управления МВД Республики Казахстан, ВУЗы и IT-сообщества

ОТКРЫТИЕ КОНФЕРЕНЦИИ		
10:00 – 10:05	offline	**Приветственное слово** **Жанат Рахимжановна Дильбарханова** Начальник Академии управления Министерства внутренних дел Республики Казахстан, доктор юридических наук, профессор, полковник полиции
10:05 – 10:10	offline	**Приветственное слово** **Эльвира Абдикапбаровна Алимова** Заместитель начальника Академии управления Министерства внутренних дел Республики Казахстан, доктор философии (PhD), ассоциированный профессор (доцент), полковник полиции
10:10 – 10:15	offline	**Приветственное слово** **Алибек Сайлауович Оразалы** Заместитель начальника Департамента по противодействию

		киберпреступности МВД Республики Казахстан, кандидат технических наук, полковник полиции
РАБОТА СЕССИИ // Доклады		
ВРЕМЯ	**ФОРМАТ УЧАСТИЯ**	**ТЕМА ДОКЛАДА И СПИКЕРЫ**
10:20 – 10:30	offline – выступления	**«Противодействие преступности в современный период: роль теории ОРД»** **Серик Жакипбекович Галиев** Кандидат юридических наук, доцент, Заслуженный работник МВД РК
10:30 – 10:40	offline – выступления	**«Некоторые аспекты международного взаимодействия в борьбе с киберпреступностью»** **Бейбит Кайратович Биржанов** Начальник 5 управления Департамента по противодействию киберпреступности МВД Республики Казахстан, полковник полиции
10:40 – 10:45	offline – выступления	**«Использование искусственного интеллекта для мониторинга и анализа контента, связанного с наркотиками, на цифровых платформах»** **Василий Владимирович Гриценко** Начальник Шестого управления Комитета по противодействию наркопреступности Министерства внутренних дел Республики Казахстан, полковник полиции
10:45 – 10:55	offline – выступления	**Деятельность TSARKA и научно-технические разработки** **Руслан Амрканович Тургульдинов** Заместитель президента ОЮЛ «Центр анализа и расследования кибератак»
10:55 – 11:05	offline – выступления	**«Оперативно-розыскная психология: проблемы и перспективы»** **Канат Саметович Лакбаев** Старший научный сотрудник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор юридических наук, профессор
11:05 – 11:15	offline – выступления	**«Использование технологий искусственного интеллекта для мониторинга средств массовой информации в целях выявления, анализа и пресечения противоправной деятельности»** **Даурен Куанышевич Рсалиев** Представитель ТОО «Seven Hills of Kazakhstan»
11:15 – 11:25	offline – выступления	**«Актуальные проблемы оперативно-розыскной деятельности: теория, законодательство и правоприменительная практика в условиях**

		цифровизации» **Мейрам Азаматович Жумабаев** ОФ «Esbol Qory» – менеджер проектов, правовед
11:25 – 11:35	**online – выступления**	**«Трансформация оперативно-розыскного противодействия молодежному экстремизму в условиях цифровизации и внедрения систем искусственного интеллекта» (на примере Республики Таджикистан)** **Абдуллозода Неъматулло Рахматулло** начальник кафедры оперативно-розыскной деятельности 4-го факультета Академии МВД Республики Таджикистан, кандидат юридических наук
11:35 – 11:40	offline – выступления	**«От реактивной модели к проактивной: искусственный интеллект в оперативно-розыскной деятельности МВД Республики Казахстан»** **Айдар Булатович Мусин** Старший научный сотрудник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор философии PhD, майор полиции
11:40 – 11:50	online – выступления	**«Проблемы использования искусственного интеллекта в оперативно-розыскной деятельности»** **Юлия Радиковна Хамзяева** начальник кафедры оперативно-розыскной деятельности Казанского юридического института МВД России кандидат юридических наук, подполковник полиции
11:50 – 12:00	**online – выступления**	**«Электронное уголовное дело: архитектура построения и адаптация для российской правовой системы»** **Моругина Надежда Анатольевна** доцент кафедры уголовного процесса Воронежского института МВД России, кандидат юридических наук, доцент, полковник полиции
12:00 – 12:30	Дискуссия, обсуждение Подведение итогов конференции Памятное фотографирование	

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясына қатысушылар
ТІЗІМІ
(offline / online)

2026 жылғы 18 қыркүйек • Астана

№ р/с	Т.А.Ә.	Қатысу форматы	Лауазымы
1.	**Жанат Рахымжанқызы Дильбарханова**	offline	Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясының бастығы, заң ғылымдарының докторы, профессор, полиция полковнигі
2.	**Эльвира Әбдіқапбарқызы Алимова**	offline	Қазақстан Республикасы Ішкі істер министрлігі Басқару академиясы бастығының орынбасары, философия докторы (PhD), қауымдастырылған профессор (доцент), полиция полковнигі
3.	**Александр Герасимович Кан**	offline	Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының бастығы, философия докторы (PhD), қауымдастырылған профессор (доцент), полиция полковнигі
4.	**Серік Жақыпбекұлы Ғалиев**	offline	Заң ғылымдарының кандидаты, доцент, Қазақстан Республикасы ІІМ-нің еңбек сіңірген қызметкері
5.	**Абдуллозода Неъматулло Рахматулло**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі кафедрасының бастығы, заң ғылымдарының кандидаты, милиция полковнигі
6.	**Бейбіт Қайратұлы Біржанов**	offline	Қазақстан Республикасы ІІМ Киберқылмысқа қарсы іс-қимыл департаментінің 5-басқармасының бастығы, полиция полковнигі
7.	**Қанат Сәметұлы Лақбаев**	offline	Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының аға ғылыми қызметкері, заң ғылымдарының докторы, профессор
8.	**Дәурен Қуанышұлы Рсалиев**	offline	«Seven Hills of Kazakhstan» ЖШС өкілі
9.	**Мейрам Азаматұлы Жұмабаев**	offline	«Esbol Qory» қоғамдық қорының жобалар менеджері, құқықтанушы
10.	**Бекжан Бекболатұлы Демесін**	offline	«Esbol Qory» қоғамдық қорының IT-маманы
11.	**Руслан Әмірқанұлы**	offline	«Кибершабуылдарды талдау және тергеу орталығы» заңды тұлғалар бірлестігі

	Тұрғұлдинов		президентінің орынбасары
12.	**Василий Владимирович Гриценко**	offline	Қазақстан Республикасы ІІМ Есірткі қылмысына қарсы іс-қимыл комитетінің 6-басқармасының бастығы, полиция полковнигі
13.	**Дулатбахит Әуезбахытұлы Рапишев**	offline	Қазақстан Республикасы ІІМ Жедел-криминалистикалық департаментінің криминалисті
14.	**Нұрбақыт Жанхан**	offline	Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының бастығы, заң ғылымдарының магистрі, полиция полковнигі
15.	**Айдар Булатович Мусин**	offline	Қазақстан Республикасы ІІМ Басқару академиясы Ғылыми-зерттеу институтының ІІО жедел-іздестіру қызметін және киберқылмысқа қарсы іс-қимылды зерттеу орталығының аға ғылыми қызметкері, философия докторы (PhD), полиция майоры
16.	**Бекхат Кенжебекұлы Қойлыбай**	offline	Қазақстан Республикасы ІІМ Экстремизмге қарсы іс-қимыл департаментінің аға жедел уәкілі, полиция майоры
17.	**Аида Батырбекқызы Базарбаева**	online	Қазақстан Республикасы ІІМ Ш.Қабылбаев атындағы Қостанай академиясының қылмыстық құқық және криминология кафедрасының бастығы, философия докторы (PhD), полиция подполковнигі
18.	**Юлия Радиковна Хамзяева**	online	Ресей ІІМ Қазан заң институтының жедел-іздестіру қызметі кафедрасының бастығы**,** заң ғылымдарының магистрі, полиция **под**полковнигі
19.	**Алексей Сергеевич Сысоев**	online	«Беларусь Республикасы Ішкі істер министрлігінің Могилев институты» білім беру Мекемесі милиция факультетінің жедел-іздестіру қызметі кафедрасының бастығы, милиция полковнигі
20.	**Ришат Талғатұлы Абенов**	online	Қазақстан Республикасы ІІМ Ш.Қабылбаев атындағы Қостанай академиясының жедел-іздестіру кафедрасының доценті, философия докторы (PhD), полиция майоры
21.	**Маннонзода Нигора Манон**	online	Тәжік мемлекеттік құқық, бизнес және саясат университеті заң факультетінің қылмыстық құқық, криминалистика және сыбайлас жемқорлыққа қарсы іс-қимыл кафедрасының доценті, заң ғылымдарының кандидаты
22.	**Абдулло Абдулло Рахматулло**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультетінің бастығы, заң ғылымдарының кандидаты, доцент, милиция подполковнигі
23.	**Ибрагимзода Джамшед Ибрагим**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі

			кафедрасының аға оқытушысы, милиция подполковнигі
24.	**Муродзода Фарход Гайрат**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі кафедрасының аға оқытушысы, милиция аға лейтенанты
25.	**Ревазода Мукаддас Рева**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі кафедрасының оқытушысы, милиция капитаны
26.	**Шарифи Махбуба Абдушукурзода**	online	Тәжікстан Республикасы ІІМ Академиясының 4-факультеті жедел-іздестіру қызметі кафедрасының кабинет бастығы, милиция аға лейтенанты
27.		offline	Қазақстан Республикасы ІІМ Басқару академиясы (жеке құрам, магистранттар және докторанттар)

СПИСОК
участников международной научно-практической конференции «Искусственный интеллект в противодействии преступности» (offline / online)

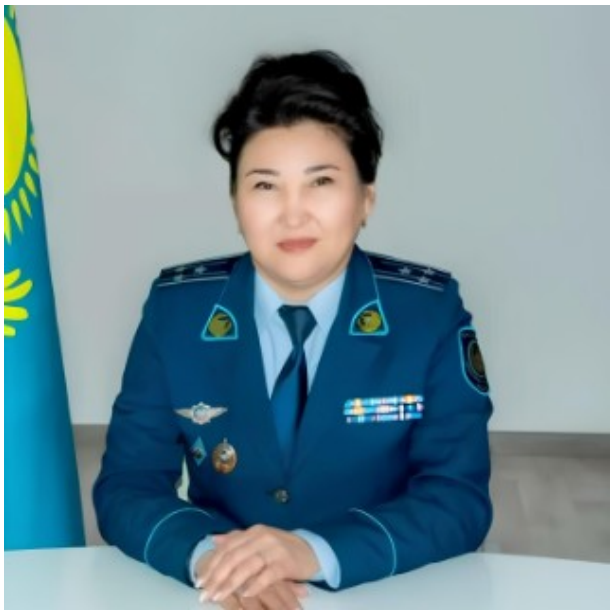
18 сентября 2026 года • Астана

№ п/н	ФИО	Формат участия	Должность
1.	**Жанат Рахимжановна Дильбарханова**	offline	Начальник Академии управления Министерства внутренних дел Республики Казахстан, доктор юридических наук, профессор, полковник полиции
2.	**Эльвира Абдикапбаровна Алимова**	offline	Заместитель начальника Академии управления Министерства внутренних дел Республики Казахстан, доктор философии (PhD), ассоциированный профессор (доцент), полковник полиции
3.	**Александр Герасимович Кан**	offline	начальник Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор философии (PhD), ассоциированный профессор (доцент), полковник полиции
4.	**Серик Жакипбекович Галиев**	offline	Кандидат юридических наук, доцент, Заслуженный работник МВД РК
5.	**Абдуллозода Неъматулло Рахматулло**	online	Начальник кафедры оперативно-розыскной деятельности 4-го факультета Академии МВД Республики Таджикистан, кандидат юридических наук, полковник милиции
6.	**Бейбит**	offline	Начальник 5 управления Департамента по

	Кайратович Биржанов		противодействию киберпреступности МВД Республики Казахстан, полковник полиции
7.	**Канат Саметович Лакбаев**	offline	Старший научный сотрудник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор юридических наук, профессор
8.	**Даурен Куанышевич Рсалиев**	offline	Представитель ТОО «Seven Hills of Kazakhstan»
9.	**Мейрам Азаматович Жумабаев**	offline	ОФ «Esbol Qory» – менеджер проектов, правовед
10.	**Бекжан Бекболатұлы Демесін**	offline	ОФ «Esbol Qory» – IT специалист
11.	**Руслан Амрканович Тургульдинов**	offline	Заместитель президента ОЮЛ «Центр анализа и расследования кибератак»
12.	**Василий Владимирович Гриценко**	offline	Начальник Шестого управления Комитета по противодействию наркопреступности Министерства внутренних дел Республики Казахстан, полковник полиции
13.	**Дулатбахит Ауезбахитович Рапишев**	offline	Криминалист оперативно-криминалистического департамента МВД Республики Казахстан
14.	**Нурбахыт Жанхан**	offline	Начальник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, магистр юридических наук, полковник полиции
15.	**Айдар Булатович Мусин**	offline	Старший научный сотрудник Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности Научно-исследовательского института Академии управления МВД Республики Казахстан, доктор философии PhD, майор полиции
16.	**Бекхат Кенжебекұлы Қойлыбай**	offline	Старший оперуполномоченный Департамента по противодействию экстремизму МВД Республики Казахстан майор полиции
17.	**Аида Батырбековна Базарбаева**	online	Начальник кафедры уголовного права и криминологии Костанайской академии МВД Республики Казахстан имени Ш.Кабылбаева, доктор философии (PhD), подполковник полиции
18.	**Юлия Радиковна Хамзяева**	online	Начальник кафедры оперативно-розыскной деятельности Казанского юридического института

			МВД России, кандидат юридических наук, подполковник полиции
19.	**Алексей Сергеевич Сысоев**	online	Начальник кафедры оперативно-розыскной деятельности факультета милиции Учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь», полковник милиции
20.	**Ришат Талгатович Абенов**	online	Доцент кафедры оперативно-розыскной деятельности Костанайской академии МВД Республики Казахстан имени Ш.Кабылбаева, доктор философии (PhD), майор полиции
21.	**Маннонзода Нигора Манон**	online	**Д**оцент кафедры уголовного права, криминалистики и противодействия коррупции юридического факультета Таджикского государственного университета права, бизнеса и политики, кандидат юридических наук
22.	**Абдулло Абдулло Рахматулло**	online	Начальник факультета № 4 Академии МВД Республики Таджикистан, к.ю.н., доцент, подполковник милиции
23.	**Ибрагимзода Джамшед Ибрагим**	online	Старший преподаватель кафедры ОРД ОВД факультета № 4 Академии МВД Республики Таджикистан, подполковник милиции
24.	**Муродзода Фарход Гайрат**	online	Старший преподаватель кафедры ОРД ОВД факультета № 4 Академии МВД Республики Таджикистан, старший лейтенант милиции
25.	**Ревазода Мукаддас Рева**	online	Преподаватель кафедры ОРД ОВД факультета № 4 Академии МВД Республики Таджикистан, капитан милиции
26.	**Шарифи Махбуба Абдушукурзода**	online	Начальник кабинета кафедры ОРД ОВД факультета № 4 Академии МВД Республики Таджикистан, старший лейтенант милиции
27.		offline	Академия управления МВД Республики Казахстан (личный состав, магистранты и докторанты)

ДИЛЬБАРХАНОВА ЖАНАТ РАХИМЖАНОВНА
Начальник Академии управления
Министерства внутренних дел Республики Казахстан,
доктор юридических наук, профессор, полковник полиции



УВАЖАЕМЫЕ КОЛЛЕГИ, УЧАСТНИКИ И ГОСТИ КОНФЕРЕНЦИИ!

От имени коллектива Академии управления Министерства внутренних дел Республики Казахстан рада приветствовать всех вас на Международной научно-практической конференции «Искусственный интеллект в противодействии преступности».

Сегодня искусственный интеллект уже стал частью практической повестки правоохранительной деятельности. Он расширяет возможности анализа информации и поддержки профессиональных решений. Вместе с тем его применение требует особой ответственности, поскольку напрямую связано с соблюдением законности, защитой прав и свобод граждан, информационной безопасностью и достоверностью результатов.

Поэтому важно оценивать не только технологические возможности искусственного интеллекта, но и условия его правомерного и безопасного использования. В центре внимания конференции — оперативно-розыскная деятельность, досудебное расследование, цифровая криминалистика, интеллектуальная обработка данных, а также правовые, организационные и этические аспекты внедрения новых решений. Такой подход позволяет рассматривать искусственный интеллект прежде всего, как инструмент повышения качества правоохранительной деятельности.

Академия управления МВД Республики Казахстан рассматривает научно-методическое сопровождение этих процессов как одно из значимых направлений

своей работы. Научные результаты должны становиться основой для методических решений и практических рекомендаций, а внедрение технологий — опираться на профессиональную экспертизу и требования законодательства.

Рассчитываю, что конференция позволит определить перспективные направления дальнейшей работы и сформировать научно-практические выводы, востребованные в исследовательской, образовательной и практической деятельности.

Благодарю всех вас за активное участие в конструктивном обмене мнениями и совместной профессиональной работе.

Желаю содержательной и плодотворной работы конференции, а также выработки обоснованных выводов и действенных предложений по обсуждаемым вопросам.

АЛИМОВА ЭЛЬВИРА АБДИКАПБАРОВНА
Заместитель начальника Академии управления Министерства внутренних дел Республики Казахстан, доктор философии (PhD), ассоциированный профессор (доцент), полковник полиции



УВАЖАЕМЫЕ КОЛЛЕГИ И ГОСТИ КОНФЕРЕНЦИИ!

Позвольте выразить признательность за участие в сегодняшней встрече, посвященной обсуждению современных возможностей применения искусственного интеллекта в противодействии преступности и перспектив его дальнейшего развития.

Сегодня цифровые технологии стремительно меняют характер преступности и одновременно расширяют возможности правоохранительных органов. Искусственный интеллект становится важным инструментом анализа данных, оперативно-розыскной деятельности, досудебного расследования и цифровой криминалистики.

Особая ценность нашей конференции заключается в объединении научного, практического и технологического опыта. Эффективное внедрение новых решений требует тесного взаимодействия правоохранительных органов, научных и образовательных организаций, государственных структур и IT-сообщества.

Не менее важен международный обмен опытом. Современные цифровые угрозы носят трансграничный характер, поэтому развитие профессионального сотрудничества и совместный поиск эффективных решений приобретают особое значение.

Для Академии важно, чтобы научные исследования и современные технологии находили практическое применение и способствовали подготовке специалистов, способных профессионально работать в условиях цифровой трансформации.

Пусть сегодняшняя конференция послужит импульсом для формирования новых научных идей, широкого распространения передового опыта и дальнейшего укрепления профессионального сотрудничества.



ГРИЦЕНКО ВАСИЛИЙ ВЛАДИМИРОВИЧ
Начальник Шестого управления
Комитета по противодействию наркопреступности
Министерства внутренних дел Республики Казахстан
полковник полиции

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ МОНИТОРИНГА И АНАЛИЗА КОНТЕНТА, СВЯЗАННОГО С НАРКОТИКАМИ НА ЦИФРОВЫХ ПЛАТФОРМАХ

УВАЖАЕМЫЕ КОЛЛЕГИ!

Цифровизация упростила сбыт и рекламу наркотиков. Организаторам наркосетей больше не нужен личный контакт с покупателем, а реклама расходится через мессенджеры и социальные сети быстрее, чем ее успевают блокировать.

Число интернет-ресурсов с наркосодержащим контентом, выявляемых Комитетом, растет кратно из года в год, и по итогам первого полугодия 2026 года эта динамика сохраняется.

Приведу общие результаты работы по основным направлениям, с показателями за оба периода. За 2025 год нами выявлено более ***34 тыс. объектов*** *информации с пропагандой или рекламой наркотиков, из которых заблокировано* ***10,5 тыс.*** *В текущем году на блокировку нами направлено более* ***15 тыс.*** *интернет-ресурсов, из них заблокировано* ***6,5 тыс*** *– процент блокировки составляет в среднем* ***от 25 до 40%.***

Параллельно мы ведем взаимодействие с представителями иностранных компаний и администрациями крупных социальных сетей и мессенджеров. Отрабатываем вопросы удаления таргетированной и иной рекламы наркотиков, а также раскрытия личности лиц, причастных к распространению противоправного контента.

По информации представителей социальных сетей, фильтрация противоправного контента на их стороне также ведется с применением искусственного интеллекта. При чем она осуществляется в основном, по ключевым словам, (курьер, закладчик и т.д.), которые им направляем мы во взаимодействии с Министерством культуры и информации.

Однако, несмотря на проводимую работу в социальных сетях, мы ежедневно выявляем все новые и новые факты распространения таргетированной наркорекламы, аккаунты и даже целые группы в мессенджерах, где предлагается трудоустройство в качестве закладчиков, курьеров и лаборантов.

В текущем году мы провели крупные задержания во взаимодействии с иностранными партнерами. В частности, совместно

с Национальной полицией Украины на территории Украины и Казахстана проведены следственно-оперативные мероприятия, направленные на установление и пресечение деятельности организаторов и участников call-центров, причастных к вербовке граждан стран Европы и Азии в качестве закладчиков, курьеров и лаборантов.

По результатам проведенных мероприятий установлены структура и механизм функционирования указанной вербовочной сети через мессенджеры и социальные сети.

Установлено, что call-центры распределены по направлениям деятельности на кадровые (которые вербуют граждан в качестве операторов) и операторские (которые вербуют граждан для работы закладчиками, курьерами и лаборантами), все они имеют единую систему управления и фактически контролируются одним лицом. При этом внутри системы действуют жесткие правила контроля. К работникам применяются значительные денежные штрафы, а в случаях нарушения установленных правил или попыток оставить работу — физическое насилие и незаконное лишение свободы.

Нами уже установлены непосредственные руководители отдельных структурных звеньев, места их дислокации и страны, с территории которых осуществляется преступная деятельность.

Основная задача этих вербовочных колл-центров — это внедрение в крупные информационные ресурсы, торговые, информационные площадки объявлений в поиске работы, то есть под видом легального трудоустройства, осуществляется реклама наркотиков и вербовка закладчиков через интернет ресурсы.

В ходе осмотра изъятой техники мы увидели, что преступники полностью мониторят информационные пространство стран, где вербуют потенциальных работников. Там есть все наши крупные сайты с поиском работы, они внедряются в общие домовые, профессиональные группы, создают анонимные аккаунты и выкидывают таргетированную рекламу.

То есть в информационном пространстве действует трансграничное преступное сообщество, которые не жалеет финансовых средств и человеческих ресурсов, для того чтобы добиться своей цели связанной с получением выгоды от реализации наркотических средств.

Соответственно, проводимая нами работа по выявлению и блокировке интернет-ресурсов в ручном режиме путём поиска через браузеры и соц. сети малоэффективна и физически не обеспечит необходимого охвата.

Без разработки программного комплекса для автоматизированного парсинга, результативность данной нормы будет оставаться очень слабой.

Рассчитываю, что настоящая конференция даст возможность продолжить эту работу совместными усилиями практиков и ученых и выработать методику применения ИИ для мониторинга и анализа наркоконтента в мессенджерах и социальных сетях.

Благодарю за внимание.



БИРЖАНОВ БЕЙБИТ КАЙРАТОВИЧ
Начальник 5 управления
Департамента по противодействию
киберпреступности МВД Республики Казахстан
полковник полиции

НЕКОТОРЫЕ АСПЕКТЫ МЕЖДУНАРОДНОГО ВЗАИМОДЕЙСТВИЯ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

УВАЖАЕМЫЕ КОЛЛЕГИ!

Сегодня международное взаимодействие в сфере противодействия киберпреступности становится одним из ключевых элементов обеспечения общественной и национальной безопасности.

Особенность киберпреступности заключается в том, что преступление может быть совершено в одной стране, инфраструктура преступников находиться в другой, потерпевшие — в третьей, а электронные доказательства храниться у поставщика цифровых услуг ещё в одной юрисдикции.

Поэтому эффективность расследования всё чаще зависит не только от возможностей национальных правоохранительных органов, но и от скорости получения информации из-за рубежа.

1. Основные проблемы международного взаимодействия

Первой проблемой остаётся ***трансграничный характер электронных доказательств****.*

В настоящее время электронные доказательства используются практически при расследовании любых категорий преступлений. INTERPOL отмечает, что цифровая криминалистика необходима для идентификации, получения, обработки и анализа данных с компьютеров, смартфонов, удалённых хранилищ и других цифровых источников.

При этом данные могут находиться за пределами государства, расследующего преступление. Получение таких данных традиционными механизмами международной правовой помощи может занимать значительное время.

В этой связи принципиальное значение имеют международные правовые инструменты, предусматривающие более оперативное получение и сохранение электронной информации.

Второй проблемой является ***различие национального законодательства и процессуальных требований****.*

Государства по-разному регулируют вопросы доступа к данным, сроков их хранения, передачи информации правоохранительным органам, защиты персональных данных и допустимости электронных доказательств в суде.

В результате действия, допустимые в одной юрисдикции, могут требовать дополнительных процедур в другой.

*Третья проблема — **скорость развития преступных технологий**.*

Europol в Internet Organised Crime Threat Assessment 2026 года отдельно выделяет шифрование, прокси-инфраструктуру и искусственный интеллект как факторы, расширяющие возможности киберпреступников. При этом в поле внимания остаются кибератаки, онлайн-мошенничество, эксплуатация детей, криптовалюты и даркнет.

Таким образом, международные механизмы сотрудничества должны развиваться с сопоставимой скоростью.

2. Формирование единой международной правовой основы

*Важным событием стало принятие Генеральной Ассамблеей ООН **Конвенции Организации Объединённых Наций против киберпреступности** 24 декабря 2024 года.*

Это первый универсальный юридически обязательный международный договор ООН, специально посвящённый киберпреступности и международному сотрудничеству в этой сфере.

Конвенция была открыта для подписания в Ханое 25–26 октября 2025 года. Казахстан, подписал Конвенцию в числе первых на торжественной церемонии в Ханое, в которой приняло участие 71 государство. По состоянию на 17 сентября 2026 года Конвенция имеет 82 подписанта и 3 государства-участника и пока не вступила в силу. Для вступления в силу требуется 40 ратификаций, принятий, утверждений или присоединений.

Особое значение имеет то, что Конвенция предусматривает механизмы международного сотрудничества и обмена электронными доказательствами по серьёзным преступлениям.

Это создаёт основу для формирования более универсального подхода к расследованию преступлений, имеющих цифровой и трансграничный характер.

*Одновременно продолжает играть важную роль **Конвенция Совета Европы о киберпреступности — Будапештская конвенция**.*

Она была открыта для подписания в 2001 году и содержит положения о криминализации компьютерных преступлений, процессуальных инструментах получения электронных доказательств и международном сотрудничестве. Её положения применяются также к расследованию других преступлений, когда электронные доказательства имеют значение для уголовного производства.

Таким образом, сегодня международное сообщество располагает несколькими правовыми механизмами, которые должны не конкурировать, а дополнять друг друга.

3. Что необходимо совершенствовать

На наш взгляд, практическое международное сотрудничество целесообразно развивать по нескольким направлениям.

Первое — сокращение времени получения электронной информации.

Для киберпреступления критически важен фактор времени. IP-адрес, данные аккаунта, сведения о транзакции или содержимое цифрового устройства могут иметь значение только при условии их своевременного сохранения.

Поэтому необходимо расширять механизмы оперативного сохранения данных и прямого взаимодействия между компетентными органами.

В рамках Будапештской конвенции уже существует сеть контактных пунктов, работающих по принципу 24/7. Второй дополнительный протокол к Конвенции направлен, в частности, на усиление международного сотрудничества и обмена электронными доказательствами. В 2026 году Совет Европы продолжает практическую работу по его реализации.

Второе — развитие единого профессионального стандарта работы с электронными доказательствами.

Необходимо обеспечить сопоставимые подходы к их изъятию, сохранению, передаче, цифровой криминалистике и документированию цепочки хранения.

Это позволит снизить риск ситуации, когда полученная в рамках международного сотрудничества информация впоследствии не может быть полноценно использована в уголовном процессе.

Третье — развитие постоянных каналов обмена оперативной информацией.

Опыт INTERPOL показывает практическую ценность постоянного обмена данными между правоохранительными органами.

INTERPOL использует Cyber Fusion Centre как механизм сбора, анализа и обмена информацией о киберугрозах, а также координирует трансграничные операции и оказывает государствам техническую и экспертную поддержку.

*Показательным примером является операция INTERPOL **Synergia**, проведённая в 2023 году с участием 60 правоохранительных органов более чем из 50 стран. В ходе операции было выявлено около 1 300 подозрительных IP-адресов и URL, а 70 процентов выявленных командных серверов были выведены из эксплуатации на момент публикации результатов.*

*Другой пример — операция **Serengeti**, проведённая INTERPOL совместно с AFRIPOL в 19 африканских странах в 2024 году. Были задержаны 1 006 подозреваемых и ликвидированы 134 089 вредоносных инфраструктур и сетей. Выявленные дела были связаны с ущербом почти в 193 миллиона долларов США.*

Эти результаты демонстрируют практическую значимость обмена оперативными данными, совместного анализа и одновременного проведения мероприятий в нескольких юрисдикциях.

4. Международное взаимодействие с частным сектором

Отдельного внимания требует взаимодействие правоохранительных органов с технологическими компаниями, финансовыми организациями, операторами связи и специалистами в сфере кибербезопасности.

Частный сектор располагает значительным объёмом технической информации, которая может использоваться для выявления преступной инфраструктуры.

INTERPOL прямо указывает на значение партнёрства правоохранительных органов с технологическими компаниями, финансовыми учреждениями и специалистами по кибербезопасности для выявления взаимосвязей между преступлениями и ускорения реагирования.

Следовательно, международное сотрудничество должно строиться не только по линии «государство — государство», но и по модели:

правоохранительные органы — международные организации — технологические компании — финансовый сектор — операторы связи — специалисты по кибербезопасности.

5. Искусственный интеллект: новые возможности и новые угрозы

Отдельно необходимо остановиться на искусственном интеллекте.

Сегодня влияние ИИ на киберпреступность имеет двусторонний характер.

С одной стороны, искусственный интеллект используется преступниками для повышения эффективности уже существующих схем.

Europol в отчёте IOCTA 2026 года рассматривает ИИ наряду с шифрованием и прокси-инфраструктурой как фактор, расширяющий возможности киберпреступности.

INTERPOL в региональной оценке угроз для Азии и Тихоокеанского региона за 2025–2026 годы также указывает на использование искусственного интеллекта, ransomware-as-a-service и сложных методов социальной инженерии в организованной киберпреступности.

С другой стороны, ИИ создаёт новые возможности для правоохранительных органов.

Он может применяться для:

- *анализа больших массивов оперативной информации;*
- *выявления взаимосвязей между цифровыми идентификаторами;*
- *обнаружения аномалий и подозрительных транзакций;*
- *анализа вредоносного программного обеспечения;*
- *автоматизированной обработки цифровых доказательств;*
- *выявления мошеннических коммуникаций;*
- *приоритизации поступающей информации;*
- *прогнозирования отдельных типов киберугроз на основе имеющихся данных.*

Практика государств уже показывает внедрение таких инструментов. Согласно оценке INTERPOL по Азии и Тихоокеанскому региону, 66,7 процента опрошенных стран сообщили о применении инструментов и систем ИИ для прогнозного анализа, цифровой криминалистики и обнаружения угроз.

При этом использование ИИ в правоохранительной деятельности требует сохранения требований к законности получения доказательств, защите персональных данных, проверяемости результатов и возможности их последующей процессуальной оценки.

*ИИ должен рассматриваться прежде всего как **инструмент поддержки сотрудника**, а не как самостоятельный источник юридически значимого решения.*

6. Практические направления дальнейшего развития

С учётом указанных проблем представляется целесообразным сосредоточить международное сотрудничество на следующих направлениях.

Первое. *Ускорить имплементацию международных договоров в национальное законодательство и обеспечить их практическое применение.*

Второе. *Развивать круглосуточные контактные пункты и прямые каналы взаимодействия между компетентными органами.*

Третье. *Создавать совместные аналитические группы для расследования транснациональных киберпреступных сетей.*

Четвёртое. *Унифицировать практику обращения с электронными доказательствами и цифровой криминалистики.*

Пятое. *Расширять государственно-частное партнёрство, прежде всего с платформами, операторами связи, финансовыми организациями и компаниями кибербезопасности.*

Шестое. *Развивать совместное использование технологий искусственного интеллекта для анализа угроз и цифровых доказательств при одновременном обеспечении законности и проверяемости результатов.*

Седьмое. *Укреплять профессиональную подготовку сотрудников правоохранительных органов, поскольку технологическое развитие преступности требует постоянного обновления компетенций.*

Современная киберпреступность является трансграничной по своей природе. Поэтому эффективность противодействия ей непосредственно связана со способностью государств быстро обмениваться информацией, сохранять электронные доказательства, проводить совместные операции и взаимодействовать с технологическим и финансовым сектором.

Создание универсальной международной правовой основы в лице Конвенции ООН против киберпреступности является важным этапом этого процесса. Одновременно сохраняют практическое значение уже действующие механизмы, включая Будапештскую конвенцию, сеть 24/7 и инструменты международного сотрудничества INTERPOL.

Следующий этап должен заключаться не только в принятии международных норм, но и в их практической реализации: сокращении сроков обмена данными, повышении совместимости национальных систем, развитии цифровой криминалистики и укреплении постоянных каналов взаимодействия.

И, наконец, искусственный интеллект одновременно изменяет возможности преступников и расширяет инструментарий правоохранительных органов.

Поэтому задача международного сообщества заключается в том, чтобы обеспечить опережающее развитие механизмов сотрудничества, технологий и профессиональных компетенций.

Только объединение правовых, оперативных, технологических и аналитических возможностей государств позволит эффективно противодействовать преступности, которая по своей природе не признаёт государственных границ.



ТУРГУЛЬДИНОВ РУСЛАН АМРКАНОВИЧ
Заместитель президента ОЮЛ «Центр анализа и расследования кибератак»

ДЕЯТЕЛЬНОСТЬ TSARKA И НАУЧНО-ТЕХНИЧЕСКИЕ РАЗРАБОТКИ

УВАЖАЕМЫЕ КОЛЛЕГИ!

Благодарю за возможность представить деятельность TSARKA, наши научные исследования и разработки. Сегодня я хотел бы показать, как накопленный нами опыт защиты информационных систем превращается в собственные технологии и как этот потенциал может быть использован в работе органов внутренних дел. Прежде всего — в исследовании цифровых следов, развитии инструментов расследования и практической подготовке специалистов.

TSARKA — Центр анализа и расследования кибератак — работает в Казахстане с 2015 года. За это время мы развили несколько взаимосвязанных направлений: анализ защищённости, мониторинг и реагирование на инциденты, разработку продуктов, научные исследования и подготовку кадров. Мы работаем с задачами защиты государственных организаций, финансового сектора, операторов связи и бизнеса.

Повседневная работа наших специалистов даёт понимание того, как происходят атаки, какими уязвимостями пользуются злоумышленники и какие следы остаются после компрометации. Этот опыт помогает формулировать задачи для разработчиков и исследователей. Для нас принципиально, чтобы научная работа отвечала на конкретный практический вопрос, а её результат можно было проверить и применить.

Коротко остановлюсь на продуктах и сервисах. TSARKA SOC обеспечивает круглосуточный мониторинг событий безопасности, выявление угроз и реагирование на инциденты. WebTotem предназначен для мониторинга и защиты веб-ресурсов. Платформа Tumar.One позволяет привлекать независимых исследователей к поиску уязвимостей в рамках согласованных программ. Эти направления дополняют друг друга: помогают заранее обнаруживать слабые места, контролировать состояние систем и своевременно разбирать возникающие инциденты.

Международные победы и призовые места TSARKA подтверждают высокий уровень казахстанской школы кибербезопасности. Наша команда TSARKA SOC добилась значимых результатов на киберучениях Cyber Drill Asia-Pacific, GISEC Cyber Drill Dubai и соревнованиях Positive Hack Days, а также заняла первое место на международных киберучениях Национального центра обмена трафиком

Беларуси. Специалисты Red Team TSARKA становились победителями и призёрами кибербитвы Standoff, неоднократно занимая первые и вторые места. В январе 2026 года наша команда под эгидой KHS — KazHackStan, представляющая Федерацию CTF Казахстана, победила в профессиональной категории международного турнира Jeanne d'Hack CTF в Руане, во Франции. Турнир объединил 363 команды со всего мира. Наши специалисты решили все 44 задания по анализу программ, поиску уязвимостей, веб-безопасности, криптографии и другим направлениям. Ещё одним достижением стало первое место объединённой студенческой команды TSARKA Kazakhstan и FR13NDS TEAM среди 26 команд на соревнованиях HackTrick в Анкаре. За этими результатами стоят навыки, непосредственно востребованные в противодействии киберпреступности: выявление атак, анализ действий злоумышленников, исследование цифровых следов и восстановление картины инцидента.

TSARKA R&D — подразделение прикладных исследований и опытно-конструкторских разработок. Оно объединяет информационную безопасность, микроэлектронику, криптографию, встраиваемые системы, сетевые технологии и цифровую криминалистику. Мы последовательно развиваем способность создавать собственные решения, понимать их устройство и адаптировать их под требования заказчика.

Команда работает по полному циклу: от постановки задачи и проектирования до создания опытных образцов, испытаний и подготовки к производству. Внутри подразделения объединены специалисты по электронике, печатным платам, системному программированию и программному обеспечению устройств. Это позволяет исследовать проблему на том уровне, где она возникает, — в алгоритме, программе или аппаратной части — и проверять решение экспериментально.

Для МВД наиболее прикладное направление — цифровая криминалистика. Мы разрабатываем модульную платформу для извлечения, восстановления и анализа данных с накопителей, видеорегистраторов систем наблюдения и мобильных устройств. Параллельно развиваются аппаратные средства работы с дисками и микросхемами памяти. По этому направлению завершаются научно-исследовательские и опытно-конструкторские работы.

Содержательная задача здесь заключается в восстановлении информации, которая недоступна при обычном просмотре: удалённых файлов, фрагментированных записей, данных со сложной внутренней структурой. Например, при исследовании видеорегистратора специалисту необходимо найти сохранившиеся фрагменты видео и установить их последовательность. Для этого нужны знания форматов хранения, алгоритмы восстановления и возможность проверить полученный результат. Именно такие задачи составляют предмет наших исследований.

Для применения в работе киберполиции предлагаем совместно определить наиболее востребованные типы устройств и сценарии исследования. На этой основе можно сформировать контрольные наборы данных и провести испытания: оценить полноту восстановления, точность результата и время работы специалиста. Такой подход позволит предметно установить, где отечественная

разработка уже полезна, а какие функции необходимо доработать под ведомственные задачи.

Другой блок R&D связан с аппаратной безопасностью. Мы развиваем направление защищённых мобильных устройств и аппаратных средств аутентификации. Tautan Secure Key — USB-ключ для многофакторной аутентификации с поддержкой FIDO2 и государственной электронной цифровой подписи. Отдельный научно-исследовательский проект посвящён отечественному криптографическому микроконтроллеру для хранения ключей и выполнения криптографических операций. Его долгосрочная ценность — развитие собственной школы проектирования компонентов безопасности.

Научная составляющая этих работ уже отражена в публикациях. Среди тем — восстановление видеодоказательств с регистраторов Hikvision и Dahua, безопасность беспроводных сетей, обнаружение угроз в сетях устройств интернета вещей и устойчивость микроконтроллеров к аппаратным воздействиям. Результаты представлены в журналах Information, Sensors, Applied Sciences, материалах конференции IEEE/ACIS и казахстанских научных изданиях. Публикации позволяют выносить методы на профессиональное обсуждение и связывать прикладную разработку с академической наукой.

Мы также развиваем специализированный научный журнал TSARKA SCIENCE. Его задача — объединить исследователей и практиков вокруг проблем информационной безопасности. В перспективе эта площадка может быть полезна для совместных работ с Академией МВД: публикации открытых результатов исследований, обсуждения методик и подготовки молодых учёных. Включение журнала в национальные и международные базы является направлением дальнейшего развития.

Особое значение для Академии МВД имеют киберполигоны. У нас уже находятся в активной эксплуатации два таких комплекса. Они объединяют виртуальную информационную инфраструктуру и интерактивный физический макет. Это позволяет воспроизводить инциденты в контролируемой среде и обучать специалистов через выполнение практических задач.

Для ведомственной подготовки мы предлагаем развивать сценарии полного цикла исследования киберинцидента: от обнаружения подозрительной активности и сбора цифровых следов до восстановления последовательности событий и подготовки технического отчёта. Один и тот же сценарий можно повторять, усложнять и использовать для оценки подготовки сотрудников. Академия могла бы определять учебные цели и методики, киберполиция — прикладные требования, а TSARKA — обеспечивать техническую реализацию и сопровождение.

Считаем перспективным выстроить сотрудничество вокруг конкретных исследовательских задач. Начать можно с испытаний платформы цифровой криминалистики и разработки учебных сценариев на киберполигоне. Для каждого направления целесообразно заранее определить ожидаемый результат и критерии оценки. Это создаст основу для совместных научных проектов и позволит переходить к внедрению по итогам проверенной практической работы.

Отдельно хочу сказать о KazHackStan. В этом году конференция проводится уже в восьмой раз. Для TSARKA это многолетняя работа по развитию профессионального сообщества. KazHackStan объединяет представителей государства, бизнеса, науки и технических команд, даёт возможность обсуждать реальные угрозы, обмениваться опытом и знакомиться с отечественными разработками. Значение конференции для страны — в укреплении связей между людьми и организациями, от которых зависит безопасность цифровой среды Казахстана.

Практическая составляющая KazHackStan помогает молодым специалистам проявить себя, а опытным командам — проверить навыки и обменяться подходами. Соревнования CyberKumbez на киберполигоне связывают обсуждение угроз с работой в моделируемой инфраструктуре. Для образовательных организаций и правоохранительных органов такая площадка представляет интерес как источник профессиональных контактов, учебных идей и знакомства с будущими кадрами отрасли.

Ещё одна инициатива связана с Международной олимпиадой по кибербезопасности — ICO. Казахстан получил право провести её в 2030 году, организатором в нашей стране выступит TSARKA. Участие в этом движении позволяет вовлекать школьников в решение практических задач и выстраивать долгосрочную подготовку кадров. Для нас это продолжение работы по развитию отечественной школы кибербезопасности.

Уважаемые коллеги!

TSARKA располагает практическим опытом, инженерной командой и научным заделом, которые могут быть полезны органам внутренних дел. Предлагаем объединить их с прикладными задачами киберполиции и научно-образовательными возможностями Академии МВД. Результатом такого взаимодействия должны стать проверенные отечественные инструменты, воспроизводимые методики исследования и специалисты, умеющие применять их в повседневной работе.

РАПИШЕВ ДУЛАТБАХИТ АУЕЗБАХИТОВИЧ
Криминалист оперативно-криминалистического департамента
МВД Республики Казахстан

КИБЕРУГРОЗЫ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ВЫЗОВЫ И ВОЗМОЖНОСТИ ДЛЯ ПОЛИЦИИ

УВАЖАЕМЫЕ КОЛЛЕГИ!

Цифровизация изменила не только повседневную жизнь граждан, но и саму природу преступности. Значительная часть мошенничеств сегодня совершается дистанционно — по телефону, в мессенджерах и социальных сетях. Одновременно стремительно развиваются технологии искусственного интеллекта, которые могут служить как преступникам, так и правоохранительным органам.

В своём докладе я остановлюсь на трёх вопросах: какие киберугрозы наиболее актуальны сегодня; что представляет собой искусственный интеллект и где он уже применяется, в том числе в полиции; насколько Казахстан готов к внедрению ИИ и что, на мой взгляд, необходимо сделать органам внутренних дел.

1. Телефонное мошенничество и социальная инженерия

Наиболее распространённая сегодня угроза — телефонные мошенники. Схема их действий типовая: злоумышленники звонят, выдают себя за сотрудников банка, полиции или КНБ, оказывают психологическое давление и просят назвать код из СМС. Получив код, они получают доступ к банковским счетам и оформляют кредиты на имя потерпевшего.

Особенно цинично выглядит практика, когда мошенники подделывают фотографии и видео руководителей правоохранительных органов и распространяют фальшивые «новости» о компенсации ущерба. Таким образом они пытаются повторно обмануть тех, кто уже стал жертвой: человек, потерявший деньги, готов заплатить за их «возврат».

Номера, с которых поступают такие звонки, нередко зарегистрированы на коммерческие структуры — ИП и ТОО, а также на старые номера банков. Это создаёт у гражданина ложное ощущение официальности звонка. Выявленные номера подлежат блокировке.

Главное средство противодействия — профилактика. Население должно чётко знать: сотрудники банка, полиции и спецслужб никогда не запрашивают коды из СМС и не просят перевести деньги на «безопасный счёт». При подозрительном звонке нужно прервать разговор и позвонить по номеру 102. И очень важно предупредить близких — прежде всего пожилых родственников.

2. Интернет-угрозы

Интернет принято делить на три уровня. Поверхностный интернет (Surface Web) — это то, что индексируют Google, Яндекс, Википедия, YouTube и социальные сети. Глубокий интернет (Deep Web) — закрытые базы данных, личные кабинеты, корпоративные и банковские системы; по распространённой оценке, именно здесь находится около 96% всего контента сети. Тёмный

интернет (Dark Web) — анонимные ресурсы, где торгуют наркотиками, похищенными данными и вредоносным программным обеспечением.

Угрозы, с которыми сталкивается рядовой пользователь, можно условно разделить на две группы. Первая связана с поведением самого человека в сети:

- *фишинг и социальная инженерия;*
- *мошенничество при интернет-покупках;*
- *социальные сети и утечка личных данных;*
- *онлайн-казино;*
- *запрещённый контент;*
- *интернет-знакомства;*
- *деструктивные сообщества и группы.*

Вторая — технические угрозы:

- *вирусы и шпионские программы;*
- *DDoS-атаки;*
- *скрытое использование чужого трафика и устройств;*
- *кража информации;*
- *атаки на банковские приложения и электронные ключи (ЭЦП);*
- *поиск и эксплуатация уязвимостей;*
- *слежка с помощью разведки по открытым источникам (OSINT).*

На последнем пункте хочу остановиться отдельно: нас изучают. Фотографии, отметки геолокации, списки друзей и номера телефонов в открытом доступе позволяют составить подробный профиль человека. Этим пользуются мошенники для подготовки целенаправленных атак. Поэтому цифровая гигиена нужна каждому, и особенно сотрудникам правоохранительных органов.

3. Кибервойна и киберволонтёры

На государственном уровне мы имеем дело уже не с отдельными преступлениями, а с фактической кибервойной. Её основные инструменты:

- ***DDoS-атаки** — нарушение работы информационных систем;*
- ***социальная инженерия** — манипуляция людьми;*
- ***взлом** — проникновение в системы;*
- ***кража информации** — для таргетирования, публикации, шантажа или продажи;*
- ***шифрование информации** — ради выкупа, уничтожения данных или их недоступности.*

Противостоять этим угрозам силами одной полиции невозможно. Поэтому мы привлекаем к работе киберволонтёров — молодых людей, которые помогают выявлять мошеннические ресурсы, запрещённый контент и ведут профилактическую работу среди сверстников. Такой формат взаимодействия с обществом считаю необходимым развивать дальше.

4. Искусственный интеллект: понятие и развитие

Идея искусственного разума давно существует в культуре. Ещё Айзек Азимов сформулировал три закона робототехники:

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинён вред.

2. Робот должен повиноваться всем приказам человека, кроме тех, что противоречат Первому закону.

3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому и Второму законам.

Сегодня эти принципы перестали быть фантастикой и стали предметом обсуждения на уровне права и этики.

Искусственный интеллект — это программирование, способное воспроизводить когнитивные способности человеческого мозга. История его развития начинается в 1950-х годах с работ Алана Тьюринга и появления самого термина «искусственный интеллект». Далее были первая программа-собеседник ELIZA (1966), экспертные системы, победа Deep Blue над Гарри Каспаровым (1997), голосовой помощник Siri (2011) и победа AlphaGo в игре го. Сегодня мы наблюдаем эпоху больших языковых моделей.

Выделяют три вида искусственного интеллекта:

*– **Слабый ИИ (Narrow AI)** решает узкие задачи: голосовые ассистенты, реклама в соцсетях, распознавание лиц. Именно такие системы используются повсеместно сегодня.*

*– **Сильный ИИ (AGI)** максимально приближен к человеческому интеллекту. По оценкам ряда экспертов, он может сформироваться к 2075 году.*

*– **Супер-ИИ (Super AI)** сможет превзойти лучшие умы человечества, самостоятельно совершенствуя свои алгоритмы.*

В основе современного ИИ лежат нейронные сети и машинное обучение. В обычной программе человек прописывает компьютеру каждую инструкцию. При машинном обучении системе дают данные, и она сама находит закономерности. Нейросеть обучается на опыте, подстраивая силу связей между нейронами: слой за слоем она выделяет признаки — контуры, формы, сочетания — и в итоге отличает, например, кошку от собаки.

Языковая модель GPT-3 была обучена на огромных массивах текстов: архивах веб-страниц (Common Crawl, WebText2), коллекциях книг и Википедии. Именно объём данных позволяет таким моделям вести осмысленный диалог.

5. Применение искусственного интеллекта

ИИ уже используется в финансах, образовании, сельском хозяйстве, промышленности, транспорте и в структурах безопасности. Остановлюсь на трёх направлениях.

***Медицина.** ИИ помогает расшифровывать снимки и кардиограммы, выявлять признаки инсульта и онкологии на ранних стадиях.*

***Правосудие.** Алгоритмы анализируют судебную практику, помогают готовить документы и снижают нагрузку на судей и сотрудников аппарата.*

***Полиция.** В ряде стран — например, в ОАЭ — уже работают роботы-полицейские, которые принимают заявления граждан и выдают справочную информацию. Широко применяются видеоаналитика, распознавание лиц и номеров, автоматическая фиксация нарушений ПДД.*

Практический опыт работы с ChatGPT

Для примера я провёл диалог с ChatGPT на профессиональную тему — ответственность за кибермошенничество в Казахстане. На просьбу выписать

конкретные статьи модель сначала перенаправляла на сайт «Әділет» (adilet.zan.kz) и лишь после нескольких уточнений дала содержательный ответ по нормам Уголовного кодекса. Не случайно в прессе писали, что ChatGPT «научился лениться и отшивать пользователей, как человек».

Вывод для нас простой: ИИ — сильный помощник, но его ответы нужно проверять по первоисточникам, особенно в правовых вопросах. При этом возможности моделей растут очень быстро: они уже создают изображения по текстовому описанию, а нейросеть OpenAI Sora — реалистичное видео. Это открывает возможности для профилактики, но и новые риски: дипфейки уже используются мошенниками.

Проект «Narkopol Comics»

Пример полезного использования генеративного ИИ — комикс ударно-целевой группы «Narkopol» Управления по противодействию наркопреступности ДП Карагандинской области. Он подготовлен в рамках Комплексного плана по борьбе с наркоманией и наркобизнесом на 2023–2025 годы (постановление Правительства от 29 июня 2023 года № 508).

Сюжет прост и понятен подростку. Группа друзей находит сумку с наркотиками и сталкивается с моральным выбором. Ребята решают отнести находку в полицию, где их благодарят за ответственность, а затем обсуждают со сверстниками опасность наркотиков. Иллюстрации созданы нейросетью в казахстанской городской среде. Такой материал изготавливается за часы, а не за недели, и не требует привлечения художников.

6. Готовность Казахстана к внедрению ИИ

В Индексе готовности правительств к искусственному интеллекту за 2023 год (Oxford Insights) Казахстан занял 72-е место из 193 стран и 3-е место в регионе Южной и Центральной Азии — после Индии и Турции.

Сильные стороны страны — доступность данных, цифровой потенциал и адаптивность правовой базы к цифровым бизнес-моделям. Слабые — отсутствие крупных частных технологических компаний, недоступность венчурного капитала и недостаточные расходы на НИОКР.

По данным Министерства науки и высшего образования, исследованиями в сфере ИИ занимаются 24 вуза и научных центра; лишь 4 вуза располагают оборудованием для обучения алгоритмов глубокого обучения (суперкомпьютеры уровня NVIDIA DGX-1). Количество научных публикаций по ИИ — 1016. Зарождаются сообщества специалистов машинного обучения, ИТ-школы и вузы включают модули по ИИ в свои программы.

Уже есть и практические результаты. В медицине — Cerebra (диагностика признаков инсульта), Smart ECG, системы ForUs Data. В сфере безопасности — система «Сергек», Единая система видеомониторинга Алматы, распознавание номеров и лиц, платформа TargetAI. В коммерческом секторе показателен пример Kolesa Group: её ИИ «Гермиона» выявляет мошеннические объявления на Kolesa.kz, Krisha.kz и Market.kz, то есть фактически решает профилактическую задачу.

Барьеры

– Низкая осведомлённость населения и бизнеса о возможностях ИИ и его отличии от простой цифровизации; как следствие — низкий спрос на разработки.

– *Качество интернета: при покрытии 99% Казахстан в индексе Speedtest занимал 73-е место из 140 по мобильному и 95-е из 181 по широкополосному доступу.*

– *Пробелы в законодательстве: на момент подготовки анализа не были закреплены понятия ИИ и технологий ИИ, отсутствовали технические стандарты, что затрудняет экспертизу таких продуктов.*

– *Нехватка инфраструктуры и вычислительных мощностей.*

– *Финансирование: созданный в 2019 году фонд поддержки исследований в сфере ИИ не функционирует в полной мере.*

– *Затруднённый доступ к данным: многие региональные и отраслевые базы не консолидированы и не структурированы.*

– *Риски безопасности: ИИ встраивается даже в детские игрушки, что создаёт угрозу утечки персональных данных.*

Международный опыт

Мировые расходы на системы ИИ по итогам 2023 года достигли 154 млрд долларов, что на 26,9% больше, чем годом ранее. С 2017 года все развитые страны утвердили национальные стратегии развития ИИ. Лидеры по инвестициям — США и Китай; среди стран ОЭСР выделяются Япония, Швеция, Германия и Франция. По прогнозу IDC, к 2025 году ИИ будет поддерживать около 90% передовых корпоративных приложений.

7. Предложение: научно-исследовательский центр ИИ при Академии полиции

С учётом сказанного предлагаю создать научно-исследовательский центр в области искусственного интеллекта при Академии полиции. Такой центр может значительно повысить эффективность и инновационность полицейских служб.

Основные направления его работы:

1. ***Междисциплинарный подход** — объединение экспертов в ИИ, криминологии и этике для разработки технологий, учитывающих права граждан.*
2. ***Партнёрство** — связи с технологическими компаниями и международными организациями для доступа к инновациям и финансированию.*
3. ***Прикладные исследования** — ИИ-решения для работы полиции, анализа данных и автоматизации рутинных процессов.*
4. ***Образовательные программы** — курсы по ИИ для сотрудников полиции всех уровней.*
5. ***Международное сотрудничество** — обмен опытом с полицейскими службами других стран.*
6. ***Инновационная инфраструктура** — современное оборудование для разработки и тестирования ИИ-приложений.*
7. ***Этические и социальные исследования** — оценка влияния ИИ на общество и защита персональных данных.*
8. ***Конференции и семинары** — обсуждение новых разработок и стандартов.*
9. ***Публикации и методические материалы** — распространение результатов исследований и рекомендаций.*

*10. **Пилотные проекты** — тестирование новых ИИ-технологий в реальных условиях.*

Заключение

Киберпреступность и искусственный интеллект развиваются параллельно. Мошенники уже используют современные технологии, и полиция не может отставать. Наши задачи — активная профилактика среди населения, развитие движения киберволонтёров, обучение сотрудников и системное внедрение ИИ в деятельность органов внутренних дел. Создание научно-исследовательского центра ИИ при Академии полиции стало бы логичным шагом в этом направлении.

Благодарю за внимание!

БАЯНДАМАЛАР
ДОКЛАДЫ

АБДУЛЛОЗОДА НЕЪМАТУЛЛО РАХМАТУЛЛО
Начальник кафедры оперативно-розыскной деятельности
4-го факультета Академии МВД Республики Таджикистан
кандидат юридических наук

ТРАНСФОРМАЦИЯ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ МОЛОДЕЖНОМУ ЭКСТРЕМИЗМУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И ВНЕДРЕНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (НА ПРИМЕРЕ РЕСПУБЛИКИ ТАДЖИКИСТАН)

Проблема молодежного экстремизма в Республике Таджикистан на протяжении последних двух десятилетий сохраняет статус одного из приоритетных направлений деятельности правоохранительных органов республики.

В течение 10 последних лет в стране выявлено и зарегистрировано 6680 преступлений, имеющих экстремистский и террористический характер. В этот период в результате активной экстремистской пропаганды посредством социальных сетей и во время пребывания в трудовой миграции граждан увеличилось число вступлений молодых людей в экстремистско-террористическую организацию «Исламское государство» и другие террористические группы, что вызывает серьезную обеспокоенность в обществе. [2, С. 9.].

Безусловно, преступления, носящие экстремистский характер, являются одними из тех видов преступлений, которые несут серьезную угрозу основам конституционного строя и безопасности государства. Все государства мира стремятся как можно скорее найти новые пути борьбы с этим нежелательным явлением общества и искоренить его. Этот опасный процесс может привести к уничтожению народностей, наций и государств [1, С. 66-69.].

Стремительное развитие информационных технологий обусловливает появление новых возможностей и способов подготовки и совершения преступлений, в том числе экстремисткой направленности [3, С. 81-84].

Одновременно с этим республика переживает интенсивную цифровую трансформацию государственного управления. Указом Президента Республики Таджикистан период 2025–2030 годов объявлен «Годами развития цифровой экономики и инноваций» [6], а постановлением Правительства от 30 сентября 2022 года № 483 утверждена Стратегия развития искусственного интеллекта в Республике Таджикистан на период до 2040 года – первый в Центральноазиатском регионе документ стратегического планирования подобного уровня [5]. Стратегия прямо предусматривает использование алгоритмов искусственного интеллекта в процессах принятия решений, государственного управления и администрирования, что создает предпосылки для их применения и в правоохранительной сфере, включая оперативно-розыскную деятельность.

Динамичное развитие информационно-телекоммуникационных технологий кардинально изменило характер современных угроз национальной безопасности Республика Таджикистан, последовательно реализующая стратегические документы в сфере противодействия терроризму и экстремизму (включая программные государственные стратегии), сталкивается с феноменом виртуализации радикальных идей.

Указанное сочетание обстоятельств формирует актуальную исследовательскую задачу: оценить, каким образом цифровизация и внедрение систем искусственного интеллекта изменяют содержание, методы и организационные формы оперативно-розыскного противодействия молодежному экстремизму, а также выявить институциональные и правовые ограничения, сдерживающие эту трансформацию в условиях Таджикистана.

Стратегия развития искусственного интеллекта в Республике Таджикистан на период до 2040 года и утвержденный первый этап плана действий на 2023–2025 годы задают институциональную рамку для внедрения алгоритмических систем в государственное управление, включая сферу общественной безопасности [5]. Согласно официальным разъяснениям, к 2030 году применение технологий искусственного интеллекта рассматривается как фактор, способный существенно повысить эффективность государственного сектора и снизить операционные издержки. В сфере оперативно-розыскной деятельности данный курс потенциально означает переход от точечного, преимущественно ручного мониторинга интернет-пространства к автоматизированной обработке больших массивов открытых и ограниченно доступных данных.

Наиболее очевидными направлениями применения технологий искусственного интеллекта в противодействии молодежному экстремизму выступают автоматизированный мониторинг открытых источников и социальных сетей с использованием алгоритмов распознавания экстремистской лексики и визуальной символики, системы видеонаблюдения с функцией распознавания лиц в местах массового пребывания граждан, а также предиктивные аналитические модели, предназначенные для оценки риска вовлечения конкретных лиц или групп в экстремистскую деятельность на основе анализа цифрового следа.

Отдельным направлением является использование алгоритмических инструментов для выявления координированной сетевой активности – ботов, фейковых аккаунтов и распределенных вербовочных кампаний, – которые сложно обнаружить методами традиционного оперативного наблюдения ввиду масштаба и скорости распространения контента.

Традиционные формы оперативного реагирования в киберпространстве исчерпывают свой ресурс, что актуализирует интеграцию интеллектуальных цифровых систем и искусственного интеллекта в деятельность оперативных подразделений.

Молодежная среда, обладающая высокой степенью цифровой вовлеченности, объективно становится главной целевой аудиторией деструктивных и международных террористических организаций. Вербовка через социальные сети, распространение завуалированного экстремистского контента и создание

латентных сетевых ячеек требуют качественного пересмотра арсенала средств и методов оперативно-розыскной деятельности.

В современных условиях трансграничный характер экстремизма проявляется в том, что вербовщики используют дистанционные каналы коммуникации, минуя физический контакт с объектами воздействия. Так, экстремисты-вербовщики используют социальные сеты, такие как Facebook, «Одноклассники», Mail.ru, Twitter, YouTube и др. для вербовки молодежи в экстремистские группировки, а также пропаганды таких групп [4, С. 57 – 58.].

Для молодежной среды Республики Таджикистан характерны следующие тенденции:

– Индивидуализация радикализации: переход от структурированных ячеек к саморадикализации одиночек под воздействием деструктивного контента в мессенджерах.

– Маскировка контента: использование криптографических средств защиты информации, локальных диалектов, метафор и элементов молодежной субкультуры для обхода базовых алгоритмов интернет-модерации.

– Трансграничность каналов финансирования и управления: координация противоправной деятельности извне с активным вовлечением трудовых мигрантов или молодежи внутри страны.

В этих реалиях перед органами осуществляющими оперативно-розыскную деятельность встает задача не просто фиксации последствий преступлений, а раннего прогнозирования и превентивного выявления скрытых деструктивных процессов.

Внедрение элементов искусственного интеллекта и предиктивной аналитики в практику оперативно-розыскной деятельности позволяет переломить ситуацию в пользу упреждающих мер. Основные направления трансформации включают:

– Создание специализированных программных комплексов, способных в режиме реального времени сканировать открытые и закрытые сегменты сети Интернет на предмет выявления признаков экстремистской идеологии. С учетом лингвистических особенностей (включая специфику таджикского языка и интернет-сленга), внедрение языковых моделей (по аналогии с развивающимися национальными инициативами в сфере искусственного интеллекта) позволяет оперативно идентифицировать маркеры радикализации в массивах текстовых, аудио- и видеоданных.

– Оперативно-розыскной анализ больших объемов обезличенных телекоммуникационных метаданных с помощью алгоритмов машинного обучения дает возможность выстраивать графы социальных связей. Это помогает обнаруживать «спящие ячейки» и локальные группы с повышенным индексом деструктивной активности еще до совершения ими противоправных деяний.

– Применение предиктивной аналитики позволяет моделировать сценарии вовлечения несовершеннолетних и молодежи в экстремистские сообщества на основе комплексных социально-демографических и поведенческих факторов, оптимизируя распределение сил и средств оперативных подразделений.

Трансформация оперативно-розыскного противодействия молодежному экстремизму в условиях цифровизации сталкивается в Таджикистане с рядом

объективных ограничений. Во-первых, законодательство об оперативно-розыскной деятельности исторически формировалось применительно к традиционным методам работы и не в полной мере учитывает специфику получения, фиксации и использования цифровых доказательств, а также правовой режим трансграничного доступа к данным, хранящимся на серверах иностранных интернет-платформ. Во-вторых, внедрение алгоритмических систем анализа поведения и коммуникации граждан порождает риск избыточного вторжения в частную жизнь и конституционные права, особенно применительно к несовершеннолетним и лицам молодого возраста, что требует выработки специальных процессуальных гарантий и механизмов судебного либо прокурорского надзора за применением подобных систем.

В-третьих, эффективное применение технологий искусственного интеллекта требует специализированной кадровой и технической инфраструктуры, подготовки аналитиков, владеющих методами обработки больших данных, специалистов по информационной безопасности и цифровой криминалистике, а также устойчивых каналов обмена данными между правоохранительными органами, оператором связи и провайдерами цифровых платформ.

В-четвертых, значительная часть цифровой инфраструктуры, используемой для распространения экстремистского контента и вербовочной коммуникации, физически и юридически находится вне национальной юрисдикции Таджикистана, что делает исключительно национальные оперативно-розыскные меры структурно недостаточными и повышает значение международного и регионального сотрудничества, в том числе в формате Содружества Независимых Государств и Шанхайской организации сотрудничества, а также двустороннего взаимодействия с государствами, на территории которых зарегистрированы крупнейшие цифровые платформы.

С учетом выявленных ограничений представляется целесообразным выделить несколько взаимосвязанных направлений совершенствования оперативно-розыскного противодействия молодежному экстремизму в условиях цифровизации. Первое направление связано с гармонизацией законодательства об оперативно-розыскной деятельности и о противодействии экстремизму с положениями Стратегии развития искусственного интеллекта, включая закрепление правового статуса автоматизированных систем анализа данных как источника оперативной информации, а не только вспомогательного технического средства, а также установление процедурных требований к фиксации и проверке результатов их работы для использования в уголовном процессе.

Второе направление предполагает развитие профилактического компонента, ориентированного не только на выявление уже сформировавшейся экстремистской активности, но и на раннее обнаружение факторов уязвимости молодежи с использованием аналитических инструментов в сочетании с традиционными формами социальной работы, образовательными и просветительскими программами.

Третье направление касается формирования специализированных подразделений и учебных программ в системе Академии МВД и профильных вузов Республики Таджикистан для подготовки сотрудников, способных работать с

методами цифровой криминалистики, анализа больших данных и мониторинга социальных сетей, а также выстраивания устойчивых межведомственных регламентов взаимодействия между Государственным комитетом национальной безопасности республики, органами внутренних дел, Агентством инноваций и цифровых технологий при Президенте Республики Таджикистан и операторами связи в части оперативного получения и обработки цифровой информации.

Четвертое направление связано с развитием международного информационного обмена и участием Таджикистана в региональных инициативах по противодействию использованию цифровых платформ в целях вербовки и пропаганды, включая согласование процедур запроса данных у зарубежных интернет-компаний и участие в совместных аналитических проектах с государствами региона Центральной Азии, сталкивающимися со сходными вызовами.

Таким образом подводя итог выше сказанному, следует отметить, что оперативно-розыскное противодействие молодежному экстремизму в Республике Таджикистан находится на начальном этапе трансформации, обусловленной общегосударственным курсом на цифровизацию и внедрение технологий искусственного интеллекта, закрепленным в Стратегии развития искусственного интеллекта на период до 2040 года и объявлением 2025–2030 годов периодом развития цифровой экономики и инноваций. Вместе с тем данная трансформация носит преимущественно рамочный, институционально-управленческий характер и пока не сопровождается специализированным правовым регулированием применения алгоритмических систем непосредственно в оперативно-розыскной деятельности.

Эффективное противодействие молодежному экстремизму в цифровой среде требует сочетания трех элементов: адаптации законодательства об оперативно-розыскной деятельности к особенностям цифровых доказательств и алгоритмического анализа данных с одновременным обеспечением гарантий прав граждан; создания специализированной кадровой и технической инфраструктуры, интегрированной с национальной стратегией развития искусственного интеллекта; и усиления международного сотрудничества в силу трансграничного характера цифровой инфраструктуры, используемой экстремистскими структурами. Только комплексная реализация данных направлений способна обеспечить соответствие оперативно-розыскной практики Республики Таджикистан характеру современных угроз молодежного экстремизма.

Список литературы:

1. Абдуллозода Н.Р. Религиозный экстремизм как угроза национальной безопасности Таджикистана. /Н.Р. Абдуллозода/ Сборник материалов III Международной научно-практической конференции на тему «Юридическая наука и практика», посвященная Дню таджикской науки и объявлению «Года правового просвещения» (г. Душанбе, 19 апреля 2024 г.) // Под ред. П.А. Насуриён. – Душанбе: Типография МВД Республики Таджикистан, 2024. С. 66-69.

2. Абдуллозода Н.Р. Современные технологии и их роль в борьбе с экстремизмом в Республике Таджикистан /Н.Р. Абдуллозода/ Проблемы и перспективы совершенствования законодательства и правоприменительной практики органов внутренних дел. Материалы дистанционной международной научно-практической конференции, приуроченной к 55-летию Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова. Караганда, 2024. С. 7-11.

3. Горбунов А.Н. Оперативно-розыскные мероприятия по выявлению преступлений экстремистской направленности в сети Интернет /А.Н. Горбунов/ Вестник Краснодарского университета МВД РОССИИ. 2021.- № 4 (54). С. 81-84.

4. Сафарзода, Х. С., Ахезода, Ш. Т., Мирзомуродзода, А. М. Пешгирии шомилшавии чавонон ба ташкилотхои экстремисти-террористи: Дастури таълими-методи. — Душанбе : Торус, 2021. С. 57 – 58.

5. Стратегия развития искусственного интеллекта в Республике Таджикистан на период до 2040 года. Утвержден постановлением Правительства от 30 сентября 2022 года № 483 (в редакции пост. Правительства РТ от 31.01.2025 №83). [Электронный ресурс] – Режим доступа: https://mmih.tj/SEARCH/DocumentView?DocumentId=143399# (дата обращения: 21.08.2026).

6. Указ Президента Республики Таджикистан Об объявлении 2025-2030 годов «Годами развития цифровой экономики и иноваций» от 08 января 2025 года № 911. [Электронный ресурс] – Режим доступа: https://mmih.tj/SEARCH/DocumentView?DocumentId=167416# (дата обращения: 21.08.2026).

АБЕНОВ АРХАТ АСЕТОВИЧ
Преподаватель факультета развития профессиональных компетенций Академии КНБ Республики Казахстан

ЦИФРОВАЯ КРИМИНАЛИСТИКА И ИНТЕЛЛЕКТУАЛЬНАЯ ОБРАБОТКА ДАННЫХ В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОМ ОБЕСПЕЧЕНИИ ПРОТИВОДЕЙСТВИЯ УГОЛОВНОЙ ПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация

Статья посвящена анализу состояния и перспектив развития цифровой криминалистики и интеллектуальной обработки данных в системе экспертно-криминалистического обеспечения противодействия уголовной преступности в Республике Казахстан. На основе открытых источников рассматриваются международные стандарты работы с цифровыми доказательствами, отечественная практика судебно-экспертных учреждений по исследованию криптоактивов, применению искусственного интеллекта для выявления синтетических медиаматериалов (дипфейков) и внедрению неинвазивных методов судебно-медицинской экспертизы. Приводятся эмпирические данные об экономико-правовой эффективности системного применения методик цифровой криминалистики. Сформулированы проблемы стандартизации, доказательственного статуса заключений, основанных на работе алгоритмов искусственного интеллекта, и направления совершенствования экспертно-криминалистической деятельности.

Ключевые слова: цифровая криминалистика; искусственный интеллект; судебная экспертиза; дипфейк; цифровые доказательства; криптоактивы; экспертно-криминалистическое обеспечение; Республика Казахстан.

Введение

Стремительная цифровизация общественных отношений закономерно сопровождается ростом числа преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также появлением качественно новых способов противодействия установлению истины по уголовным делам – от сокрытия следов в облачных хранилищах и криптовалютных транзакциях до фальсификации доказательств средствами генеративного искусственного интеллекта. В этих условиях традиционный криминалистический инструментарий, ориентированный на материальные следы, оказывается недостаточным, что и обусловило формирование цифровой криминалистики как самостоятельного научно-практического направления, интегрирующего криминалистику, компьютерные науки и стандарты информационной безопасности.

Целью статьи является анализ современного состояния экспертно-криминалистического обеспечения противодействия уголовной преступности в Республике Казахстан в части интеллектуальной обработки цифровых данных, а также определение проблем, сдерживающих внедрение соответствующих технологий в судебно-экспертную практику.

1. Цифровая криминалистика как научно-практическое направление: понятие, стандарты, статус цифровых доказательств

В отечественной научной литературе цифровая криминалистика характеризуется как область, занимающаяся исследованием и сбором доказательств в цифровом формате при расследовании преступлений, связанных с компьютерами, электронными устройствами и сетью Интернет; отмечается её тесная связь с кибербезопасностью, поскольку цифровые преступления эксплуатируют уязвимости информационных систем, а её дальнейшее развитие напрямую зависит от прогресса технологий искусственного интеллекта, анализа больших данных и криптографии.

Комплексное теоретико-методологическое исследование данного направления применительно к казахстанской следственной практике проведено в статье коллектива авторов Т.Ш. Бисембиева, А.А. Бекбауовой и Л.А. Мурсаловой, опубликованной в 2026 году в «Вестнике Актюбинского регионального университета имени К. Жубанова». В работе рассмотрены правовой статус цифровых доказательств, принцип сохранения доказательственной цепочки («chain of custody»), классификация программно-аппаратных комплексов, а также соотнесена отечественная практика с международными стандартами ISO/IEC 27037, руководством ACPO по надлежащей практике работы с электронными доказательствами и методическими рекомендациями NIST SP 800-86 по интеграции криминалистических методов в реагирование на инциденты. Ключевым эмпирическим результатом исследования, основанным на статистике цифровых преступлений в Казахстане за 2018–2023 годы, стал вывод о том, что системное применение методик цифровой криминалистики позволяет сократить средние сроки расследования на 65,8 % при одновременном повышении раскрываемости соответствующих преступлений до 89 %, что подтверждает правовую и экономическую целесообразность дальнейшего реформирования данной сферы.

Практическую реализацию данного направления в Казахстане обеспечивают специализированные экспертные организации, оказывающие услуги компьютерно-технической экспертизы и цифровой криминалистики (форензики), включая идентификацию электронных доказательств, поиск и юридически корректное закрепление цифровых следов, e-Discovery, OSINT и IT-аудит информационных систем в соответствии с международным стандартом ISO 21043, что свидетельствует о постепенной институционализации этого вида экспертной деятельности наряду с традиционными государственными судебно-экспертными учреждениями.

2. Интеллектуальная обработка данных в исследовании криптоактивов и цифровых финансовых следов

Одним из наиболее динамично развивающихся прикладных направлений цифровой криминалистики в Казахстане стало экспертное исследование операций с цифровыми (крипто-) активами. Как сообщили в Центре судебных экспертиз Министерства юстиции Республики Казахстан, с октября 2025 года в рамках уголовных дел применяется специальная методика, позволяющая вычислять доходы от операций с криптовалютой и отслеживать связанные с ними банковские переводы. Данный инструментарий имеет прямое значение для противодействия

легализации преступных доходов, мошенничеству с использованием криптоактивов и иным формам киберпреступности, при расследовании которых установление движения денежных средств традиционными методами существенно затруднено анонимностью распределённых реестров.

По сведениям того же ведомства, следующим этапом развития методической базы должна стать работа с продуктами нейросетей: исследование дипфейков, иного нейросетевого контента и специфических киберпреступлений в настоящее время прорабатывается совместно с правоохранительными и специальными государственными органами, которые определяют соответствующие экспертные потребности. Такой подход отражает общую логику опережающего реагирования судебно-экспертной системы на появление новых, технологически сложных способов совершения и сокрытия преступлений.

3. Искусственный интеллект в выявлении синтетических медиаматериалов и модернизация судебно-медицинской экспертизы

Отдельного внимания заслуживает внедрение в Казахстане методики судебно-фонографического исследования, позволяющей выявлять признаки применения технологий искусственного интеллекта в аудиозаписях типа deepfake. Директор Центра судебных экспертиз Министерства юстиции Республики Казахстан Бакытжан Байтилесов на пресс-конференции отметил, что данная методика существенно расширяет возможности судебно-фонографических исследований и способствует повышению качества экспертной оценки, а также эффективности установления подлинности аудиоматериалов, имеющих доказательственное значение по уголовным делам. Появление подобного инструментария закономерно обусловлено лавинообразным распространением синтетических медиаматериалов, создаваемых при помощи генеративных моделей, что по экспертным оценкам делает автоматизированную, основанную на алгоритмах ИИ детекцию единственно жизнеспособным способом противодействия использованию дипфейков в доказывании по уголовным, гражданским и административным делам.

Технологическая модернизация затрагивает и судебно-медицинскую экспертизу: в Казахстане внедряется метод неинвазивного исследования, известный как виртуальное вскрытие, для чего обновлены стандарты оснащения лабораторий, а наличие компьютерного томографа, позволяющего устанавливать причины смерти без хирургического вмешательства, стало обязательным требованием. Одновременно практика указывает на сохраняющуюся значимость традиционных методов верификации: известны случаи, когда только после эксгумации и повторной экспертизы устанавливались телесные повреждения, полученные потерпевшим ещё при жизни, что подчёркивает необходимость сочетания цифровых и классических криминалистических методов, а не полной замены одних другими.

4. Проблемы стандартизации и направления совершенствования экспертно-криминалистического обеспечения

Анализ приведённых практик позволяет выделить ряд системных проблем. Во-первых, отсутствует единообразное закрепление доказательственного статуса заключений, полученных с использованием алгоритмов искусственного интеллекта

(в том числе при детекции дипфейков и анализе криптотранзакций), что порождает риск оспаривания таких заключений стороной защиты по мотиву непрозрачности алгоритма. Во-вторых, требуется формирование межведомственной методической базы, единой для органов внутренних дел, прокуратуры и судебно-экспертных учреждений, поскольку исследование нейросетевого контента, как отмечают представители Центра судебных экспертиз, пока находится на стадии совместной проработки потребностей, а не завершённой методики. В-третьих, актуальна проблема междисциплинарных компетенций экспертов: цифровые следы требуют одновременного владения методами традиционной криминалистики и современными программно-техническими средствами, что предполагает пересмотр программ подготовки и переподготовки судебных экспертов. В-четвёртых, ведомство прямо признаёт необходимость нахождения баланса между полнотой и обоснованностью экспертных заключений, с одной стороны, и соблюдением разумных процессуальных сроков экспертиз – с другой, что особенно значимо при использовании ресурсоёмких методов (виртуальное вскрытие, многоуровневый анализ синтетических медиаматериалов).

Принятие профильного Закона Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII, закрепившего риск-ориентированный подход и обязательную сертификацию систем искусственного интеллекта, применяемых в сфере правосудия, создаёт предпосылки для решения части указанных проблем – прежде всего в части подтверждения надёжности алгоритмов, используемых судебно-экспертными учреждениями. Вместе с тем процессуальное законодательство (Уголовно-процессуальный кодекс Республики Казахстан) пока не содержит специальных норм о порядке назначения, производства и оценки экспертиз, основанных на технологиях искусственного интеллекта, что оставляет пространство для дальнейших научных исследований и законотворческой работы.

Заключение

Проведённый анализ показывает, что экспертно-криминалистическое обеспечение противодействия уголовной преступности в Республике Казахстан переживает этап интенсивной технологической модернизации: внедрены методики исследования криптоактивов и дипфейк-аудиозаписей, обновляются стандарты судебно-медицинской экспертизы, а научные исследования подтверждают значительный экономико-правовой эффект системного применения цифровой криминалистики. В то же время дальнейшее развитие данного направления требует: во-первых, законодательного закрепления процессуального статуса и порядка оценки заключений, основанных на работе алгоритмов искусственного интеллекта; во-вторых, разработки единой межведомственной методической базы исследования нейросетевого контента; в-третьих, приведения программ подготовки судебных экспертов в соответствие с международными стандартами (ISO/IEC 27037, NIST SP 800-86, ACPO) и требованиями к междисциплинарным компетенциям; в-четвёртых, выработки нормативов, обеспечивающих разумный баланс между полнотой экспертного исследования и процессуальными сроками. Комплексная реализация данных мер позволит повысить доказательственную ценность результатов

цифровой криминалистики и укрепить научно-техническую основу противодействия уголовной преступности в Республике Казахстан.

Список литературы:

1. Бисембиев Т.Ш., Бекбауова А.А., Мурсалова Л.А. Цифровая криминалистика: особенности современной методики расследования // Вестник Актюбинского регионального университета имени К. Жубанова. 2026. Т. 84. № 2. С. 400–408. DOI: 10.70239/arsu.2026.t84.n2.47. URL: https://vestnik.arsu.kz/index.php/hab/article/view/912 (дата обращения: 03.09.2026).

2. Как в Казахстане развивается цифровая криминалистика [Электронный ресурс] // el.kz. URL: https://el.kz/ru/kak-v-kazahstane-razvivaetsya-tsifrovaya-kriminalistika_77382/ (дата обращения: 03.09.2026).

3. Компьютерно-техническая экспертиза и цифровая криминалистика [Электронный ресурс] // Центр компьютерной и программно-технической экспертизы (ЦКПТЭ). URL: https://ccste.kz/ (дата обращения: 03.09.2026).

4. Виртуальное вскрытие и анализ дипфейков: как в Казахстане меняют судебную экспертизу [Электронный ресурс] // Bizmedia.kz. 19.05.2026. URL: https://bizmedia.kz/2026-05-19-virtualnoe-vskrytie-i-analiz-dipfejkov-kak-v-kazahstane-menyayut-sudebnuyu-ekspertizu/ (дата обращения: 03.09.2026).

5. В Казахстане используется новая методика выявления использования ИИ в дипфейках [Электронный ресурс] // Bizmedia.kz. 13.05.2026. URL: https://bizmedia.kz/2026-05-13-v-kazahstane-ispolzuetsya-novaya-metodika-vyyavleniya-ispolzovaniya-ii-v-dipfejkah/ (дата обращения: 03.09.2026).

6. Экспертиза РК усилила контроль подлинности аудио с применением ИИ [Электронный ресурс] // Otyrar.kz. URL: https://otyrar.kz/2026/05/ekspertiza-rk-usilila-kontrol-podlinnosti-audio-s-primeneniem-ii/ (дата обращения: 03.09.2026).

7. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК [Электронный ресурс] // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 03.09.2026).

8. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. Geneva: ISO, 2012.

9. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg: NIST, 2006. 121 p. DOI: https://doi.org/10.6028/NIST.SP.800-86.

10. ACPO (Association of Chief Police Officers). Good Practice Guide for Computer-Based Electronic Evidence. Version 5. London: ACPO, 2012.

АБЕНОВ РИШАТ ТАЛГАТОВИЧ
Доцент кафедры оперативно-розыскной деятельности
Костанайской академии МВД Республики Казахстан
имени Ш.Кабылбаева,
доктор философии (PhD), майор полиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И ДОСУДЕБНОМ РАССЛЕДОВАНИИ

Современный этап развития информационных технологий характеризуется быстрым внедрением искусственного интеллекта (далее – ИИ) в различные сферы государственной и общественной деятельности. Правоохранительная деятельность в данном отношении не является исключением. Увеличение объемов цифровой информации, распространение преступлений, совершаемых с использованием информационно-коммуникационных технологий, появление новых способов сокрытия следов преступной деятельности обусловливают необходимость применения более совершенных методов обработки и анализа данных. В этих условиях технологии ИИ способны существенно изменить подходы к оперативно-розыскной деятельности, досудебному расследованию и информационно-аналитическому обеспечению противодействия преступности.

Актуальность рассматриваемой проблемы для Республики Казахстан определяется не только технологическим развитием, но и формированием самостоятельной нормативной базы в сфере ИИ. 17 ноября 2025 года принят Закон Республики Казахстан № 230-VIII ЗРК «Об искусственном интеллекте», определивший основные правовые и организационные основы регулирования соответствующих общественных отношений [1]. Закон закрепляет такие принципы государственного регулирования в сфере ИИ, как законность, справедливость и равенство, прозрачность и объяснимость, ответственность и подконтрольность, приоритет благополучия человека и свободы его воли, защита данных и конфиденциальность, безопасность и защищенность. Важно, что законодатель уже ориентирует развитие ИИ не исключительно на технологическую эффективность, а на соблюдение прав и законных интересов человека.

Для правоохранительной сферы это положение имеет принципиальное значение. Оперативно-розыскная деятельность и досудебное расследование связаны с возможностью ограничения отдельных прав и свобод человека исключительно на основаниях и в порядке, установленных законом. Поэтому внедрение ИИ в данные сферы не может рассматриваться только как вопрос технической модернизации. Оно требует определения четких пределов допустимого использования алгоритмических систем, порядка контроля за их функционированием и юридического значения результатов, полученных с их помощью.

Закон Республики Казахстан от 15 сентября 1994 года «Об оперативно-розыскной деятельности» определяет правовые основы осуществления оперативно-розыскных мероприятий, их задачи, содержание и гарантии законности [2]. В

условиях цифровизации преступности традиционные методы получения и обработки оперативной информации объективно дополняются цифровыми инструментами. При этом принятие в 2025 году специального Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации» свидетельствует о том, что законодатель уже начал адаптацию отраслевого законодательства к новым технологическим условиям [3].

Особенность использования ИИ в оперативно-розыскной деятельности заключается в способности современных систем обрабатывать значительные объемы информации и устанавливать взаимосвязи между данными, которые при обычном человеческом анализе могут оставаться незамеченными. Например, алгоритмические инструменты могут применяться для систематизации сведений об объектах оперативного интереса, анализа цифровых следов, выявления устойчивых связей между лицами, телефонными номерами, транспортными средствами, электронными аккаунтами и финансовыми операциями. Значительный потенциал имеется также в автоматизированном анализе видеоматериалов, обработке текстовой информации и выявлении аномальных моделей поведения.

Однако сама способность алгоритма обнаруживать определенную закономерность не означает установления юридически значимого факта. В этом заключается одна из наиболее существенных проблем использования ИИ в правоохранительной деятельности. Алгоритм может сформировать вероятностный вывод, однако вероятность не может автоматически подменять доказанность обстоятельства, предусмотренную уголовно-процессуальным законом. Поэтому результат работы системы ИИ должен рассматриваться прежде всего как инструмент информационно-аналитической поддержки сотрудника, а не как самостоятельное основание для принятия решения, затрагивающего права человека.

Данный подход особенно важен применительно к досудебному расследованию. Уголовно-процессуальный кодекс Республики Казахстан устанавливает систему процессуальных гарантий, порядок собирания, исследования и оценки доказательств, а также полномочия участников уголовного процесса [4]. Внедрение ИИ в расследование может значительно ускорить поиск информации, анализ документов и электронных данных, установление связей между различными объектами и формирование следственных версий. Вместе с тем законодательство должно четко разграничивать технический результат работы информационной системы и доказательство по уголовному делу.

Представляется недопустимым положение, при котором заключение алгоритма автоматически приобретает доказательственное значение исключительно в силу того, что оно сформировано технологически сложной системой. Любой результат применения ИИ должен быть проверен уполномоченным должностным лицом с учетом требований уголовно-процессуального законодательства. Более того, при использовании ИИ необходимо обеспечивать возможность установления источников данных, использованных системой, времени их обработки, примененных алгоритмов и лица, ответственного за использование полученного результата.

Особое значение приобретает проблема объяснимости алгоритмических решений. Современные системы машинного обучения способны формировать результаты, логика которых не всегда очевидна даже специалисту, непосредственно работающему с системой. Для коммерческих или вспомогательных информационных сервисов такая особенность может иметь ограниченное значение. Однако в правоохранительной деятельности ситуация принципиально иная. Если результат работы алгоритма влияет на выбор направления расследования, проведение оперативного мероприятия или оценку лица, должна существовать возможность установить, почему система сформировала именно такой вывод.

Именно поэтому закрепленный в статье 7 Закона Республики Казахстан «Об искусственном интеллекте» принцип прозрачности и объяснимости имеет особое значение для правоохранительной деятельности. Пользователь системы должен иметь информацию о ее характеристиках и ограничениях, а лицо, в отношении которого принимается решение с использованием ИИ, в предусмотренных законом случаях должно иметь возможность получить информацию о процедуре автоматизированной обработки и способах защиты своих прав. Это формирует необходимую основу для последующего развития специальных норм, регулирующих применение ИИ правоохранительными органами.

Другим существенным вопросом является защита персональных данных. Использование ИИ в ОРД и расследовании предполагает обработку значительных массивов информации, в том числе сведений о физических лицах. Закон Республики Казахстан «О персональных данных и их защите» устанавливает правовые основы сбора, обработки и защиты персональных данных [5]. При использовании ИИ соответствующие требования приобретают дополнительное значение, поскольку алгоритмическая обработка позволяет объединять и сопоставлять сведения из различных источников значительно быстрее, чем традиционные методы обработки информации.

Следовательно, наличие технической возможности объединить различные массивы данных еще не означает наличие правового основания для такого объединения. Для каждого случая применения ИИ должны быть определены законная цель обработки, правовое основание, допустимый объем данных, порядок доступа к ним и требования к их защите. Особую опасность представляет использование избыточных либо недостоверных данных, поскольку ошибка, содержащаяся в исходной информации, может быть автоматически распространена на большое количество последующих аналитических решений.

С этой проблемой тесно связана опасность алгоритмической дискриминации. Если система обучается на исторических данных, содержащих определенные статистические перекосы, она способна воспроизводить эти перекосы в своих результатах. Например, если в исходном массиве данных определенные категории лиц или территории исторически чаще фигурировали в материалах правоохранительных органов, алгоритм может ошибочно интерпретировать данную статистическую связь как признак повышенной вероятности совершения преступления. В результате может возникнуть риск формирования необоснованного подозрения в отношении лица только на основании косвенных характеристик.

Для правоохранительной деятельности подобная ситуация является принципиально недопустимой. Законодательство Республики Казахстан прямо закрепляет принцип справедливости и равенства при создании и эксплуатации систем ИИ и предусматривает необходимость исключения дискриминации. Следовательно, использование ИИ в противодействии преступности должно строиться на качественных, репрезентативных и проверенных данных, а результаты алгоритмического анализа – подвергаться обязательной профессиональной оценке.

В данном контексте представляет интерес международный опыт. Европейская комиссия по эффективности правосудия Совета Европы (CEPEJ) еще в 2018 году приняла Европейскую этическую хартию по использованию ИИ в судебных системах и их окружении. В документе сформулированы пять основных принципов: уважение фундаментальных прав, недопущение дискриминации, качество и безопасность, прозрачность и справедливость, а также принцип контроля со стороны пользователя [6]. Хотя Хартия непосредственно относится к судебным системам, сформулированные в ней подходы имеют значение и для правоохранительной деятельности, поскольку отражают общую проблему использования алгоритмических технологий в сфере правосудия.

Особого внимания заслуживает именно принцип «под контролем пользователя». Его содержание заключается в том, что ИИ должен выступать инструментом профессиональной деятельности, а пользователь сохраняет возможность понимать, оценивать и контролировать результаты его работы. Для правоохранительной сферы данный принцип целесообразно трансформировать в обязательное правило: решение, способное повлечь юридически значимые последствия для человека, не должно приниматься исключительно на основании автоматизированного алгоритмического вывода.

Вместе с тем нельзя отрицать значительный практический потенциал ИИ. Наиболее оправданным представляется его использование на первоначальных и аналитических этапах работы. В частности, ИИ может применяться для интеллектуального поиска информации, автоматической классификации документов, выявления совпадений и взаимосвязей, анализа цифровых массивов, обработки видеоматериалов, построения графов связей и подготовки аналитических справок. В таком случае система не заменяет сотрудника, а сокращает время на выполнение технически сложных операций и позволяет сосредоточить профессиональные ресурсы на оценке полученной информации.

Перспективным является использование ИИ для криминологического и оперативно-аналитического прогнозирования. Анализ пространственно-временных характеристик преступности может позволить выявлять устойчивые закономерности и определять направления профилактической работы. Однако прогнозирование должно использоваться именно как аналитический инструмент. Нельзя допускать автоматического переноса вероятностной оценки на конкретное лицо и тем более принятия в отношении него ограничительных мер исключительно на основании статистического прогноза.

В этой связи представляется необходимым сформировать специальный механизм ведомственного контроля за применением ИИ в правоохранительных органах Республики Казахстан. Такой механизм должен включать обязательную

регистрацию случаев использования ИИ, определение ответственного должностного лица, фиксацию использованных информационных ресурсов, сохранение результатов работы системы и возможность последующего аудита. При этом должна обеспечиваться возможность установить, какое решение было сформировано системой, какое решение принял сотрудник и по каким причинам сотрудник согласился либо не согласился с рекомендацией алгоритма.

Особое значение имеет вопрос ответственности. Закон «Об искусственном интеллекте» закрепляет принцип ответственности и подконтрольности и предусматривает обязанность владельца, обладателя и/или пользователя обеспечивать постоянный контроль за системой ИИ в зависимости от их роли на различных этапах ее жизненного цикла [1]. Для правоохранительной сферы данный принцип необходимо наполнить конкретным содержанием. Использование ИИ не должно создавать ситуацию, при которой должностное лицо освобождается от ответственности ссылкой на ошибку алгоритма. Напротив, внедрение ИИ должно сопровождаться четким распределением ответственности между разработчиком, владельцем системы, администратором и непосредственным пользователем.

С учетом изложенного представляется целесообразным разработать специальный ведомственный нормативный акт, регулирующий использование технологий ИИ в оперативно-служебной деятельности правоохранительных органов. В нем необходимо определить допустимые направления применения ИИ, категории решений, которые не могут приниматься исключительно автоматизированным способом, требования к качеству данных, порядок документирования результатов алгоритмической обработки, процедуру проверки достоверности результатов и правила проведения периодического аудита систем.

Одновременно необходимо определить минимальные требования к профессиональной подготовке сотрудников, использующих ИИ. Недостаточно предоставить сотруднику доступ к технологическому инструменту. Он должен понимать принципы функционирования системы, ее ограничения, вероятность ошибок, особенности формирования результатов и способы их проверки. В противном случае существует риск так называемого «автоматизационного смещения», когда пользователь начинает воспринимать рекомендацию системы как заведомо правильную только вследствие ее технологического характера.

Таким образом, внедрение ИИ в оперативно-розыскную деятельность и досудебное расследование следует рассматривать как комплексный правовой, организационный и технологический процесс. Его эффективность определяется не количеством внедренных цифровых систем, а способностью обеспечить сочетание технологических преимуществ с требованиями законности и защиты прав человека.

Для Республики Казахстан на современном этапе представляется наиболее обоснованной модель, при которой ИИ используется прежде всего для обработки и анализа информации, выявления взаимосвязей, формирования аналитических материалов и поддержки профессиональной деятельности сотрудников. При этом юридически значимое решение должно оставаться результатом деятельности уполномоченного должностного лица, которое несет ответственность за его законность и обоснованность.

В конечном итоге основным принципом применения ИИ в правоохранительной деятельности должен стать принцип «искусственный интеллект помогает принимать решение, но не подменяет лицо, ответственное за его принятие». Именно такое разграничение позволит использовать технологический потенциал ИИ для повышения эффективности противодействия преступности, одновременно сохраняя фундаментальные гарантии законности, справедливости, равенства и защиты прав человека.

Список литературы:

1. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК (с изменениями и дополнениями по состоянию на 24 июня 2026 года) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://adilet.zan.kz/rus/docs/Z2500000230.

2. Об оперативно-розыскной деятельности: Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII (с изменениями и дополнениями по состоянию на 24 июня 2026 года) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://www.adilet.zan.kz/rus/docs/Z940004000_.

3. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации: Закон Республики Казахстан от 17 ноября 2025 года № 231-VIII ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://www.adilet.zan.kz/rus/docs/Z2500000231.

4. Уголовно-процессуальный кодекс Республики Казахстан: Кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК (с изменениями и дополнениями по состоянию на 12 августа 2026 года) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://www.adilet.zan.kz/rus/docs/K1400000231.

5. О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 года № 94-V (с изменениями и дополнениями) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://adilet.zan.kz/rus/docs/Z1300000094.

6. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment: adopted by the European Commission for the Efficiency of Justice (CEPEJ) at its 31st plenary meeting, Strasbourg, 3–4 December 2018. Strasbourg: Council of Europe, 2018. Electronic resource: Council of Europe – CEPEJ European Ethical Charter.

7. О кибербезопасности: Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК (с изменениями и дополнениями) // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». Электронный адрес: https://adilet.zan.kz/rus/docs/Z1500000418.

АЙДАРОВА АЙДАНА АЙДАРҚЫЗЫ
Офицер факультета развития профессиональных компетенций
Академии КНБ Республики Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ УГОЛОВНОЙ ПРЕСТУПНОСТИ: ОПЫТ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И ДОСУДЕБНОМ РАССЛЕДОВАНИИ РЕСПУБЛИКИ КАЗАХСТАН

Аннотация

В статье рассматриваются состояние, практика и перспективы применения технологий искусственного интеллекта (далее – ИИ) в противодействии уголовной преступности в Республике Казахстан. Анализируется формирующаяся нормативно-правовая база – Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII и сопутствующий Закон № 231-VIII, а также действующее законодательство об оперативно-розыскной деятельности. На основе открытых источников исследуются конкретные примеры внедрения ИИ в деятельность Министерства внутренних дел и Генеральной прокуратуры Республики Казахстан: цифровой (интерактивный) помощник следователя в Информационной системе «Единый реестр досудебных расследований», видеоаналитические комплексы и биометрическая идентификация. Определены проблемные вопросы правового, организационного и этического характера, сформулированы предложения по совершенствованию законодательства и правоприменительной практики.

Ключевые слова: искусственный интеллект; оперативно-розыскная деятельность; досудебное расследование; цифровизация правоохранительной деятельности; видеоаналитика; распознавание лиц; правовое регулирование искусственного интеллекта; цифровая криминалистика; Республика Казахстан.

Введение

Уголовная преступность на современном этапе всё активнее перемещается в цифровую среду и приобретает трансграничный, высокотехнологичный характер, что снижает эффективность традиционных методов оперативно-розыскной деятельности и досудебного расследования. Одновременно стремительное развитие технологий искусственного интеллекта – систем машинного обучения, компьютерного зрения, обработки естественного языка – открывает правоохранительным органам качественно новые инструменты предупреждения, выявления и раскрытия преступлений. Данная тенденция характерна не только для развитых правопорядков, но и для Республики Казахстан, где на государственном уровне взят курс на цифровизацию правоохранительной системы.

Значимость темы для Казахстана подтверждается тем, что Главой государства объявлен год цифровизации и искусственного интеллекта, в рамках которого Генеральная прокуратура Республики Казахстан приступила к внедрению технологий ИИ в сферу уголовного процесса, заключив меморандумы о

сотрудничестве с отечественными IT-компаниями и организациями цифровой экосистемы в целях реализации совместных цифровых проектов и внедрения отечественных технологических решений в деятельность специальных прокуроров.

Целью настоящей статьи является анализ текущего состояния нормативно-правового регулирования и правоприменительной практики использования искусственного интеллекта в оперативно-розыскной деятельности, досудебном расследовании и информационно-аналитическом обеспечении противодействия преступности в Республике Казахстан, а также выявление сопутствующих правовых, организационных и этических проблем.

1. Нормативно-правовые основы применения искусственного интеллекта в правоохранительной сфере Республики Казахстан

Правовую основу оперативно-розыскной деятельности в Казахстане по-прежнему составляет Закон «Об оперативно-розыскной деятельности» от 15 сентября 1994 года № 154-XIII, неоднократно изменявшийся, в том числе в связи с вопросами цифровизации. Вместе с тем именно 2025–2026 годы стали переломными для правового регулирования искусственного интеллекта как такового.

17 ноября 2025 года Президент Республики Казахстан подписал профильный Закон «Об искусственном интеллекте» № 230-VIII, вступивший в силу 18 января 2026 года. Данный акт впервые в национальном праве закрепляет понятийный аппарат, принципы безопасности, прозрачности и ответственности при разработке и эксплуатации систем ИИ, а также распределяет компетенцию Правительства и государственных органов в этой сфере, вводит институт оператора национальной платформы искусственного интеллекта и относит уполномоченным органом Министерство искусственного интеллекта Республики Казахстан. Закон закрепляет риск-ориентированный подход к регулированию: системы ИИ, применяемые в сферах правосудия, медицины и транспорта, отнесены к категории высокого риска и подлежат обязательной сертификации, тогда как для систем среднего риска предусмотрены требования к информированию пользователей, а для низкорисковых сфер – добровольные стандарты.

Одновременно был принят сопутствующий Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации» от 17 ноября 2025 года № 231-VIII, вступивший в силу по истечении шестидесяти календарных дней после официального опубликования, то есть с 17 января 2026 года, которым скорректирован массив смежного законодательства. Реализация обоих законов сопровождается изданием подзаконных актов: распоряжением Премьер-Министра от 14 января 2026 года № 2-р утверждён перечень правовых актов, принятие которых обусловлено новым регулированием.

Важным для правоприменительной практики является разъяснение Верховного Суда Республики Казахстан о том, что при причинении вреда системой искусственного интеллекта ответственность несёт оператор такой системы при отсутствии вины пользователя, что закладывает основу для распределения ответственности и в случаях использования ИИ правоохранительными органами.

Несмотря на принятие профильного Закона об ИИ, ни он, ни Закон «Об оперативно-розыскной деятельности», ни Уголовно-процессуальный кодекс не содержат пока специальных норм, регламентирующих порядок использования продуктов работы ИИ (транскриптов допросов, аналитических прогнозов, результатов видеоаналитики и биометрической идентификации) в качестве ориентирующей или доказательственной информации, а также порядок их проверки и оспаривания. Данный пробел представляет собой открытый вопрос теории и законодательства оперативно-розыскной деятельности и требует самостоятельного научного осмысления.

2. Практика внедрения искусственного интеллекта в оперативно-розыскную деятельность и досудебное расследование

Наиболее развёрнутым примером внедрения ИИ в досудебное расследование в Казахстане является запущенный Министерством внутренних дел проект интерактивного (цифрового) помощника следователя, встроенного в Информационную систему «Единый реестр досудебных расследований». Система включает четыре ключевых модуля – планирование расследования, обработку показаний, подготовку процессуальных документов, а также аналитику и прогнозирование. Функционально она способна переводить речь в текст, сопоставлять показания разных лиц и выявлять содержащиеся в них противоречия, предлагать следователю уточняющие вопросы для проведения допроса и автоматически формировать процессуальные документы. В тестовом режиме система с 19 июня 2025 года применяется Управлением полиции района Есиль города Астаны, а её последующее внедрение было анонсировано в отделе полиции города Косшы Акмолинской области. Ожидаемый эффект – сокращение времени расследования и снижение нагрузки на следователей за счёт автоматизации рутинных операций.

На уровне Генеральной прокуратуры цифровизация уголовного процесса реализуется как самостоятельное направление: по поручению Генерального прокурора проведены рабочие встречи с представителями IT-компаний и цифровой экосистемы, подписаны меморандумы о совместных цифровых проектах, обмене опытом и внедрении отечественных технологических решений в деятельность специальных прокуроров, при этом ИИ рассматривается как дополнительный инструмент расследования уголовных дел в русле принципа «Закон и порядок».

Параллельно развивается направление профилактики правонарушений средствами видеоаналитики. В Алматы в местах массового отдыха внедрены камеры с искусственным интеллектом, способные распознавать лица, фиксировать драки, скопления людей и признаки агрессивного поведения, а также отдельные административные нарушения; проект реализован в рамках объявленного года профилактики. Ещё более показательным примером является применение в Карагандинской области робота-полицейского («робособаки») с функцией распознавания лиц в режиме реального времени: уже в первые дни эксплуатации с её помощью были выявлены лицо, уклонявшееся от уплаты алиментов, двое должников по исполнительным производствам и ранее судимое лицо, нарушившее установленное судом ограничение на пребывание вне жилища. Подобные системы «безопасного/умного города» также используются для розыска пропавших без

вести и лиц, объявленных в розыск: при совпадении изображения с ориентировкой информация автоматически передаётся дежурным нарядам полиции, а видеоаналитика дополнительно фиксирует подозрительные предметы, скопления людей и конфликтные ситуации, требующие реагирования.

Отдельного внимания заслуживает применение ИИ для противодействия распространению наркотиков через интернет-платформы. В научной литературе отмечается, что технологии искусственного интеллекта способны существенно повысить точность и оперативность принятия решений правоохранительными органами при расследовании интернет-наркопреступлений, однако для этого необходимо создание специальной нормативной базы, которая обеспечила бы одновременно эффективность расследований и соблюдение прав человека.

3. Цифровая криминалистика и информационно-аналитическое обеспечение противодействия преступности

По сравнению с направлением автоматизации следственной работы, применение ИИ непосредственно в экспертно-криминалистической деятельности в Казахстане на сегодняшний день носит менее выраженный, точечный характер и в значительной степени остаётся перспективным направлением. Международный и уже частично казахстанский опыт видеоаналитики (распознавание лиц, транспортных средств, силуэтов и поведенческих паттернов, поиск по видеоархивам) показывает потенциал технологий компьютерного зрения для формирования цифровых доказательств и информационно-аналитического сопровождения расследования организованной и серийной преступности. Развитие этого направления в Казахстане потребует интеграции ведомственных баз данных, стандартизации форматов цифровых следов и подготовки специалистов, владеющих методикой применения соответствующих инструментов при производстве судебных экспертиз.

В теоретическом плане важно учитывать, что статус оперативно-розыскной деятельности как самостоятельной отрасли права остаётся предметом научной дискуссии: в литературе рассматриваются позиции от признания её подотраслью уголовного процесса до обоснования отраслевой самостоятельности, что обусловлено закреплённым в Законе «Об оперативно-розыскной деятельности» и институте негласных следственных действий дуализмом правового регулирования. Отмечается также, что внедрение искусственного интеллекта на стадии досудебного расследования способно содействовать реализации ключевых функций теории оперативно-розыскной деятельности – доктринально-регулятивной, методологической, интегративной, прогностической, охранительной и институционально-развивающей, что подчёркивает необходимость согласованного развития теории, законодательства и цифровых технологий.

4. Правовые, организационные и этические риски внедрения искусственного интеллекта в правоохранительную деятельность

Расширение практики видеомониторинга и биометрической идентификации порождает устойчивую общественную дискуссию о балансе между безопасностью и неприкосновенностью частной жизни. Ещё в проекте нормативного акта, опубликованном на портале «Открытые НПА», предлагалось организовать видеоаналитику на стороне национальной системы видеомониторинга с

интеграцией с базами разыскиваемых и состоящих на учёте лиц, включая идентификацию по походке, профилю лица и голосу. Эксперты указывают, что подобные возможности одновременно повышают раскрываемость правонарушений и создают риск избыточного проникновения государства в частную жизнь граждан, что требует чётких правовых гарантий и ограничений при использовании таких систем.

К числу основных рисков применения ИИ в оперативно-розыскной деятельности и досудебном расследовании следует отнести: вероятность ошибок первого и второго рода при биометрической идентификации (ложные срабатывания и пропуски); непрозрачность алгоритмов («эффект чёрного ящика»), затрудняющую проверку обоснованности выводов ИИ в состязательном процессе; накопление и хранение больших массивов биометрических и иных персональных данных, требующее усиленных мер защиты в соответствии с законодательством о персональных данных; отсутствие устоявшейся практики проверки и оспаривания стороной защиты продуктов работы ИИ; а также риск дискриминационного смещения алгоритмов в отношении отдельных социальных групп.

Принятие Закона «Об искусственном интеллекте» с его риск-ориентированным подходом, требованием обязательной сертификации систем высокого риска и закреплённой ответственностью оператора системы за причинённый вред является значимым шагом к снижению перечисленных рисков. Вместе с тем для правоохранительной сферы целесообразна разработка специализированных отраслевых стандартов – в том числе методик тестирования алгоритмов на отсутствие дискриминации, о необходимости которых упоминается применительно к сфере искусственного интеллекта в целом, – а также создание механизма независимого аудита систем ИИ, используемых органами внутренних дел и прокуратуры, и системы профессиональной подготовки сотрудников по вопросам этичного и правомерного применения таких систем.

Заключение

Проведённый анализ показывает, что Республика Казахстан находится на начальном, но динамичном этапе интеграции технологий искусственного интеллекта в систему противодействия уголовной преступности. За относительно короткий период сформирована базовая нормативно-правовая основа – Закон «Об искусственном интеллекте» № 230-VIII и сопутствующий Закон № 231-VIII, – а на практике уже функционируют или проходят пилотную апробацию конкретные инструменты: цифровой помощник следователя в системе «Единый реестр досудебных расследований», видеоаналитические комплексы профилактики правонарушений, роботизированные системы патрулирования с функцией распознавания лиц.

Вместе с тем сохраняется существенный разрыв между темпами технологического внедрения и степенью детализации отраслевого (уголовно-процессуального и оперативно-розыскного) регулирования порядка использования, проверки и оспаривания результатов работы ИИ. В связи с этим представляется целесообразным: во-первых, дополнить Закон «Об оперативно-розыскной деятельности» и Уголовно-процессуальный кодекс Республики Казахстан нормами, определяющими правовой статус и порядок использования продуктов ИИ в

оперативно-розыскной и следственной практике; во-вторых, разработать ведомственные методики и этические стандарты применения ИИ, включая обязательное тестирование алгоритмов на дискриминационные искажения; в-третьих, сформировать механизм независимого аудита и общественного контроля за системами видеонаблюдения и биометрической идентификации; в-четвёртых, развивать направление цифровой криминалистики и информационно-аналитического обеспечения расследования организованной преступности; в-пятых, обеспечить системную подготовку и переподготовку кадров правоохранительных органов по вопросам применения технологий искусственного интеллекта. Реализация данных предложений позволит гармонично сочетать повышение эффективности противодействия уголовной преступности с гарантиями прав и свобод человека, что и составляет главную задачу цифровой трансформации правоохранительной системы Республики Казахстан.

Список литературы:

1. Об оперативно-розыскной деятельности: Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII (с изменениями и дополнениями) [Электронный ресурс]. URL: https://base.spinform.ru/show_doc.fwx?rgn=1269 (дата обращения: 03.09.2026).

2. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК [Электронный ресурс] // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 03.09.2026).

3. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации: Закон Республики Казахстан от 17 ноября 2025 года № 231-VIII ЗРК [Электронный ресурс]. URL: https://pro1c.kz/news/zakonodatelstvo/izmeneniya-v-soputstvuyushchem-zakonodatelstve-po-voprosam-tsifrovizatsii-i-iskusstvennogo-intellekt/ (дата обращения: 03.09.2026).

4. О мерах по реализации законов Республики Казахстан от 17 ноября 2025 года «Об искусственном интеллекте» и «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации»: Распоряжение Премьер-Министра Республики Казахстан от 14 января 2026 года № 2-р [Электронный ресурс] // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/R2600000002 (дата обращения: 03.09.2026).

5. Принят Закон Республики Казахстан «Об искусственном интеллекте» [Электронный ресурс] // EY в Казахстане. URL: https://www.ey.com/ru_kz/technical/tax-alerts/2025/12/law-on-artificial-intelligence-kazakhstan (дата обращения: 03.09.2026).

6. Оралбаев Ч. Ключевые аспекты Закона Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК [Электронный ресурс] // PRG.KZ. URL: https://prg.kz/document/?doc_id=33297881 (дата обращения: 03.09.2026).

7. Московчук А. ИИ поможет следователям Казахстана раскрывать преступления [Электронный ресурс] // Zakon.kz. 20.06.2025. URL: https://www.zakon.kz/sobytiia/6481595-ii-pomozhet-sledovatelyam-kazakhstana-raskryvat-prestupleniya.html (дата обращения: 03.09.2026).

8. Новая глава в расследованиях: Казахстан внедряет ИИ в уголовный процесс [Электронный ресурс] // Azattyq Rýhy. URL: https://rus.azattyq-ruhy.kz/society/113127-novaia-glava-v-rassledovaniiakh-kazakhstan-vnedriaet-ii-v-ugolovnyi-protsess (дата обращения: 03.09.2026).

9. В Казахстане впервые задействовали робособаку с ИИ для охраны общественного порядка [Электронный ресурс] // Zakon.kz. URL: https://www.zakon.kz/amp/sobytiia/6525225-v-kazakhstane-vpervye-zadeystvovali-robosobaku-s-ii-dlya-okhrany-obshchestvennogo-poryadka.html (дата обращения: 03.09.2026).

10. Камеры с ИИ видеоаналитикой запустили для повышения безопасности в барах Алматы [Электронный ресурс] // BES.media. URL: https://bes.media/news/kameri-s-ii-videoanalitikoy-zapustili-dlya-povisheniya-bezopasnosti-v-barah-almati-c88958/ (дата обращения: 03.09.2026).

11. Система распознавания лиц в Казахстане: тотальная слежка или борьба с преступниками? [Электронный ресурс] // Azattyq Rýhy. URL: https://rus.azattyq-ruhy.kz/analytics/13303-sistema-

raspoznavaniia-lits-v-kazakhstane-totalnaia-slezhka-ili-borba-s-prestupnikami (дата обращения: 03.09.2026).

12. Умный город: как технологии делают жизнь безопаснее и комфортнее [Электронный ресурс] // Казахстанская правда. URL: https://kazpravda.kz/n/umnyy-gorod-kak-tehnologii-delayut-zhizn-bezopasnee-i-komfortnee/ (дата обращения: 03.09.2026).

13. Олейник В. Использование возможностей искусственного интеллекта в борьбе с интернет-наркопреступлениями в Казахстане // Академические исследования в современной науке. [Электронный ресурс]. URL: https://inlibrary.uz/index.php/arims/article/view/129862 (дата обращения: 03.09.2026).

14. Место и роль оперативно-розыскной деятельности в системе правовых наук // Вестник Академии правоохранительных органов. [Электронный ресурс]. URL: https://vestnikacademy.elpub.ru/jour (дата обращения: 03.09.2026).

15. Закон об искусственном интеллекте в Казахстане 2025 [Электронный ресурс] // Femida-Justice. URL: https://femida-justice.com/pravovye-materialy/zakon-ob-iskusstvennom-intellekte-v-kazaxstane/ (дата обращения: 03.09.2026).

АХМЕТОВ КАЗБЕК РАИМБЕКОВИЧ
Доцент кафедры факультета развития профессиональных компетенций Академии КНБ Республики Казахстан
магистр психологии

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ АНАЛИЗА ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ В КАЗАХСТАНЕ

Цифровизация общественных отношений сопровождается не только расширением использования информационных технологий, но и увеличением количества цифровых следов, возникающих в процессе повседневной деятельности пользователей и функционирования информационных систем. Современное киберпреступление может оставлять следы одновременно на различных цифровых объектах: компьютерах и мобильных устройствах, серверах, в сетевом трафике, электронных сообщениях, облачных хранилищах и финансовых системах. В результате расследование преступлений в цифровой среде все чаще связано с необходимостью обработки значительных объемов разнородной информации.

Особенность цифровых следов заключается в их высокой изменчивости, распределенности и взаимосвязанности. Один фрагмент информации, рассматриваемый изолированно, может не иметь существенного криминалистического значения, тогда как сопоставление нескольких цифровых следов способно позволить восстановить последовательность событий и установить взаимосвязи между субъектами, устройствами и цифровыми объектами. В этих условиях традиционный ручной анализ сталкивается с ограничениями, связанными прежде всего с объемом информации и необходимостью оперативного установления скрытых закономерностей.

Одним из перспективных инструментов решения данной проблемы является искусственный интеллект. Технологии машинного обучения и интеллектуального анализа данных позволяют автоматизировать поиск и классификацию информации, выявлять аномальные события, устанавливать взаимосвязи между цифровыми объектами и содействовать реконструкции последовательности действий при расследовании компьютерных инцидентов. При этом использование ИИ не предполагает замены специалиста, а направлено на повышение скорости и эффективности его аналитической работы.

Для Республики Казахстан данная проблематика приобретает особое значение в связи с развитием цифровой криминалистики и формированием соответствующих профессиональных компетенций. В современных нормативных документах уже предусматриваются функции специалистов, связанные с анализом цифровых данных, исследованием сетевого трафика, цифровых устройств и реконструкцией событий компьютерных инцидентов. В этой связи внедрение интеллектуальных инструментов может рассматриваться как перспективное направление дальнейшего развития цифрового криминалистического обеспечения расследований.

Вместе с тем применение ИИ при исследовании цифровых следов связано с рядом ограничений. Ошибочная интерпретация цифровой информации, зависимость алгоритмов от качества исходных данных, проблема объяснимости результатов и необходимость обеспечения целостности исследуемых данных требуют сохранения профессионального контроля со стороны специалиста. Поэтому вопрос заключается не только в том, насколько эффективно ИИ способен анализировать цифровые следы, но и в том, каким образом его результаты должны использоваться в криминалистической деятельности.

Цифровой след представляет собой информацию, возникающую в результате использования цифровых устройств, информационных систем и сетевых сервисов и потенциально имеющую значение для установления обстоятельств совершенного преступления. В отличие от традиционных материальных следов, цифровая информация может существовать одновременно в нескольких информационных средах, быстро изменяться, копироваться и удаляться. Это делает ее ценным, но одновременно сложным объектом криминалистического исследования.

При расследовании киберпреступлений цифровые следы могут формироваться на компьютерах и мобильных устройствах, серверах, в электронной почте и мессенджерах, сетевом трафике, браузерах, облачных хранилищах, информационных системах и финансовых сервисах. В совокупности они способны содержать сведения о времени совершения действий, используемом устройстве, характере взаимодействия с информационной системой и последовательности операций.

Особенность цифровых следов заключается в том, что их криминалистическое значение часто определяется не отдельным элементом, а совокупностью взаимосвязанных данных. Например, IP-адрес сам по себе не обязательно позволяет установить лицо, совершившее определенное действие. Однако его сопоставление со временем подключения, характеристиками устройства, данными учетной записи и другими цифровыми событиями может позволить сформировать более полную картину произошедшего.

В связи с этим одной из основных задач цифровой криминалистики становится не только обнаружение и сохранение отдельных цифровых объектов, но и установление взаимосвязей между различными цифровыми следами. Именно здесь возникают предпосылки для применения искусственного интеллекта, способного обрабатывать большие массивы информации и выявлять закономерности, которые сложно обнаружить посредством последовательного ручного анализа.

Искусственный интеллект может существенно расширить возможности цифровой криминалистики прежде всего за счет автоматизации обработки больших массивов информации. При расследовании киберпреступления специалисту приходится работать с данными различного типа и происхождения, часть которых может иметь непосредственное значение для установления обстоятельств события, а часть — не содержать криминалистически значимой информации. В таких условиях алгоритмический анализ позволяет сократить объем первичной обработки и сосредоточить внимание специалиста на наиболее релевантных объектах.

Одним из основных направлений является **автоматизированный поиск и классификация цифровых данных**. ИИ может использоваться для обнаружения файлов, сообщений, сетевых событий и других объектов по заданным признакам, а также для их группировки и предварительной классификации. Это особенно важно при исследовании больших объемов информации, когда последовательный ручной просмотр всех объектов требует значительного времени.

Вторым направлением выступает **установление взаимосвязей между цифровыми следами**. Алгоритмические инструменты способны сопоставлять временные характеристики событий, сведения об устройствах, учетных записях, сетевых соединениях и других объектах. В результате отдельные фрагменты информации могут быть объединены в единую последовательность, позволяющую сформировать более целостное представление о механизме киберпреступления.

Третьим перспективным направлением является реконструкция событий компьютерного инцидента. На основании данных из различных источников ИИ может содействовать восстановлению временной последовательности действий и определению взаимосвязи между отдельными событиями. Это позволяет перейти от исследования разрозненных цифровых объектов к реконструкции предполагаемого механизма преступления.

При этом результат алгоритмической реконструкции должен рассматриваться именно как аналитическая модель события, требующая проверки специалистом. ИИ способен предложить наиболее вероятную последовательность действий на основании имеющейся информации, однако он не может самостоятельно гарантировать достоверность каждого элемента такой реконструкции.

Одним из наиболее перспективных направлений применения искусственного интеллекта в цифровой криминалистике является реконструкция событий, связанных с совершением киберпреступления. В отличие от простого поиска отдельных цифровых следов, реконструкция предполагает установление их временной последовательности и взаимосвязи. Это позволяет перейти от набора разрозненных данных к целостной модели произошедшего события.

При расследовании киберпреступления цифровые следы могут формироваться одновременно в нескольких информационных системах. Одно действие пользователя способно оставить информацию на конечном устройстве, сервере, в журнале сетевого оборудования, облачном сервисе или иной системе. Поэтому одной из задач специалиста становится синхронизация этих сведений и установление последовательности действий.

ИИ способен содействовать решению данной задачи посредством автоматизированного сопоставления временных меток, идентификаторов устройств, сетевых параметров и других характеристик цифровых объектов. На этой основе может формироваться временная линия инцидента, позволяющая определить последовательность действий и возможные переходы между отдельными этапами преступления.

При этом принципиально важно различать реконструкцию события и установление виновности конкретного лица. Алгоритм может выявить определенную последовательность цифровых действий, однако наличие связи

между цифровым объектом и конкретным человеком требует дополнительной проверки. Использование одного алгоритмического вывода без подтверждения другими источниками информации способно привести к ошибочной интерпретации.

Поэтому наиболее рациональной является модель, в которой ИИ формирует аналитическую реконструкцию, а специалист проверяет ее на соответствие имеющимся цифровым данным и иным обстоятельствам расследования. Такой подход позволяет использовать высокую скорость алгоритмической обработки, сохраняя профессиональную оценку человека.

Для цифровой криминалистики Казахстана развитие такого подхода представляется перспективным, поскольку позволяет повысить эффективность исследования больших объемов цифровой информации и сократить время, необходимое для восстановления механизма компьютерного инцидента. При этом ключевым условием остается сохранение проверяемости каждого этапа реконструкции и недопущение автоматической подмены экспертного вывода результатом работы алгоритма.

Несмотря на значительный потенциал искусственного интеллекта, его применение при анализе цифровых следов связано с рядом ограничений, которые необходимо учитывать при расследовании киберпреступлений. Основная проблема заключается в том, что высокая скорость обработки информации сама по себе не гарантирует достоверности полученного результата. Алгоритмический вывод всегда зависит от качества исходных данных, используемой модели и корректности ее интерпретации.

Другим ограничением является зависимость ИИ от полноты исследуемого массива. Если часть цифровых следов была удалена, повреждена либо изначально недоступна для исследования, алгоритм может сформировать неполную или ошибочную реконструкцию события. Поэтому отсутствие определенной информации не должно автоматически интерпретироваться системой как отсутствие соответствующего события.

Особое значение имеет **обеспечение целостности цифровых данных**. При криминалистическом исследовании необходимо обеспечить сохранность исходной информации и возможность установить, какие действия осуществлялись с цифровым объектом в процессе его анализа. Использование ИИ не отменяет этих требований. Напротив, при автоматизированной обработке необходимо дополнительно фиксировать примененные инструменты, параметры исследования и полученные результаты.

Проблему представляет и недостаточная объяснимость некоторых алгоритмических моделей. Если система выявила определенную взаимосвязь или сформировала реконструкцию события, специалист должен иметь возможность понять основания такого вывода. Результат, который невозможно проверить или воспроизвести, ограничивает его криминалистическую ценность.

Кроме того, существует риск чрезмерного доверия специалиста к результатам ИИ. Автоматизированная система может восприниматься как более объективная по сравнению с человеком, однако алгоритм также способен ошибаться. Поэтому результат интеллектуального анализа должен рассматриваться как один из

элементов исследования, требующий сопоставления с другими цифровыми следами и обстоятельствами дела.

Для Казахстана это означает необходимость не только внедрения интеллектуальных инструментов в цифровую криминалистику, но и формирования соответствующих методических подходов к их применению. Специалист должен обладать возможностью установить происхождение исследуемых данных, последовательность их обработки и основания формирования алгоритмического результата. Только при соблюдении этих условий использование ИИ может стать инструментом повышения качества расследования, а не дополнительным источником неопределенности.

Развитие цифровой криминалистики в Казахстане создает предпосылки для более широкого применения интеллектуальных технологий при расследовании киберпреступлений. Профессионализация соответствующей деятельности и увеличение объема цифровой информации требуют не только подготовки специалистов, но и внедрения инструментов, способных ускорить обработку и сопоставление цифровых данных. В этой связи ИИ может рассматриваться как дополнительный технологический ресурс цифрового криминалистического обеспечения.

Подобная организация позволяет разделить техническую обработку больших массивов информации и профессиональную криминалистическую оценку. ИИ может выполнять наиболее ресурсоемкие операции по поиску и сопоставлению данных, тогда как специалист определяет их значение с учетом обстоятельств расследования.

Важным направлением является развитие компетенций специалистов по цифровым технологиям. Использование ИИ требует сочетания знаний в области криминалистики, информационной безопасности, анализа данных и искусственного интеллекта. Специалист должен не только уметь использовать соответствующий программный инструмент, но и понимать ограничения алгоритма, возможные источники ошибок и способы проверки полученного результата.

Перспективным также является развитие специализированных отечественных решений, ориентированных на особенности казахстанской правоохранительной практики. Такие системы могут учитывать специфику используемых информационных ресурсов, национального законодательства и организации расследования. При этом разработка подобных инструментов должна сопровождаться требованиями к безопасности, защите данных, воспроизводимости результатов и контролю со стороны специалистов.

Отдельного внимания требует методическое обеспечение использования ИИ. Необходимо определить единые подходы к документированию алгоритмического анализа, фиксации исходных данных, описанию применяемых инструментов и интерпретации полученных результатов. Это позволит повысить сопоставимость результатов различных исследований и снизить риск субъективного или некорректного использования алгоритмических выводов.

Проведенный анализ показывает, что цифровые следы становятся одним из ключевых источников криминалистически значимой информации при расследовании киберпреступлений. Их распределенность между различными

устройствами, информационными системами и сетевыми ресурсами, а также значительный объем формируемых данных существенно усложняют традиционный процесс исследования.

Искусственный интеллект способен повысить эффективность цифровой криминалистики за счет автоматизации поиска и классификации информации, выявления взаимосвязей между цифровыми объектами, анализа сетевых данных и реконструкции последовательности событий. Наиболее значимым представляется использование ИИ не для замены специалиста, а для сокращения объема рутинной аналитической работы и повышения скорости обработки больших массивов цифровых данных.

Для цифровой криминалистики принципиальное значение имеют целостность, проверяемость и воспроизводимость результатов исследования. Использование интеллектуальных технологий должно сопровождаться документированием исходных данных, применяемых инструментов и последовательности аналитических операций. Это необходимо для того, чтобы полученный результат мог быть проверен и интерпретирован специалистом.

В условиях Казахстана перспективным направлением является формирование интеллектуально усиленной модели цифровой криминалистики, объединяющей современные технологии искусственного интеллекта с профессиональными компетенциями специалистов по цифровым технологиям. Такая модель предполагает использование ИИ на этапах поиска, обработки и сопоставления информации при сохранении за специалистом функции криминалистической оценки.

В дальнейшем развитие данного направления целесообразно связывать с совершенствованием технологий интеллектуального анализа, подготовкой специалистов, разработкой методических стандартов применения ИИ и обеспечением надежности и воспроизводимости результатов цифровых криминалистических исследований.

Список литературы:

1. **Об искусственном интеллекте**: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК (с изменениями и дополнениями по состоянию на 24 июня 2026 года). – URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 18.08.2026).

2. **О персональных данных и их защите**: Закон Республики Казахстан от 21 мая 2013 года № 94-V (с изменениями и дополнениями по состоянию на 12 июля 2026 года). – URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 18.08.2026). Закон действительно имеет обновленную редакцию; последняя зафиксированная дата изменения — 12 июля 2026 года.

3. **Уголовно-процессуальный кодекс Республики Казахстан**: Кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. – URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 18.08.2026).

4. **ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме**. – М.: Стандартинформ, 2015. – 28 с. Стандарт является национальным принятием ISO/IEC 27037:2012 и регулирует идентификацию, сбор, получение и сохранение потенциально значимых цифровых свидетельств.

5. Kent K., Chevalier S., Grance T., Dang H. **Guide to Integrating Forensic Techniques into Incident Response**. – Gaithersburg: National Institute of Standards and Technology, 2006. – 121 p. – (NIST Special Publication 800-86). – DOI: 10.6028/NIST.SP.800-86.

6. **Digital forensics and strong AI: A structured literature review** // Forensic Science International: Digital Investigation. – 2023. – Vol. 46. – Art. 301617. – DOI: 10.1016/j.fsidi.2023.301617. В статье систематически рассматривается современное состояние исследований применения ИИ в цифровой криминалистике.

7. **Artificial intelligence in mobile forensics: A survey of current status, a use case analysis and AI alignment objectives** // Forensic Science International: Digital Investigation. – 2024. – Vol. 49. – Art. 301737. – DOI: 10.1016/j.fsidi.2024.301737.

8. Garach J., Singh S. K., R. N., Reddy A. P. C., Khan H. **A Comprehensive Review on Artificial Intelligence in Digital Forensics With Taxonomies, Issues, and Solutions** // Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning / ed. P. Goel. – Hershey: IGI Global, 2024. – P. 1–28. – DOI: 10.4018/979-8-3693-6557-1.ch001.

9. **Practitioner-driven framework for AI adoption in digital forensics** // Forensic Science International: Digital Investigation. – 2025. – Vol. 55. – Art. 302030. – DOI: 10.1016/j.fsidi.2025.302030. Работа непосредственно рассматривает практическое внедрение ИИ в цифровую криминалистику, включая вопросы стандартизации, прозрачности и практических ограничений.

10. Zamil M. Z. H., Khan T. M. **AI-Driven Digital Evidence Triage in Digital Forensics: A Comprehensive Review** // 2025 13th International Symposium on Digital Forensics and Security (ISDFS). – 2025. – DOI: 10.1109/ISDFS65363.2025.11011908. Работа посвящена применению ИИ для первичной сортировки и анализа цифровых доказательств.

БАЗАРБАЕВА АИДА БАТЫРБЕКОВНА
Начальник кафедры уголовного права и криминологии
Костанайской академии МВД Республики Казахстан
имени Ш.Кабылбаева
доктор философии (PhD), подполковник полиции

ВОЗМОЖНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОФИЛАКТИКЕ ПРАВОНАРУШЕНИЙ И СОВЕРШЕНСТВОВАНИИ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

На современном этапе общественного развития коррупция остается одной из наиболее устойчивых и разрушительных угроз безопасности, эффективности государственного управления и верховенства закона. Коррупционные проявления снижают уровень доверия населения к государственным институтам, ослабляют правопорядок и способствуют росту социально-экономических рисков. Особую остроту данная проблема приобретает в органах внутренних дел (ОВД), где наличие властных и контрольных полномочий у сотрудников создает предпосылки для злоупотреблений и подрывает основы профессиональной этики правоохранительной службы.

Одновременно с этим стремительное развитие информационно-коммуникационных и цифровых технологий формирует принципиально новые возможности для повышения прозрачности, контроля и аналитического сопровождения деятельности государственных органов. Применение таких инструментов, как большие данные (Big Data), искусственный интеллект (ИИ), интеллектуальные системы видеонаблюдения, электронный документооборот и цифровые регистры служебного поведения, позволяет автоматизировать процессы, минимизировать влияние человеческого фактора и повысить подотчетность правоохранительных органов.

В условиях цифровой трансформации особое значение приобретает модернизация правоохранительной деятельности. В соответствии с Указом Президента Республики Казахстан Касым-Жомарта Токаева № 1151 от 6 января 2026 года 2026 год объявлен Годом цифровизации и искусственного интеллекта [1]. Данное решение отражает стратегический курс государства на внедрение цифровых и интеллектуальных технологий во все сферы государственного управления, включая систему органов внутренних дел, что открывает новые возможности для усиления антикоррупционных механизмов.

В рамках государственной политики в Казахстане реализуются инициативы, направленные на цифровую трансформацию ОВД: автоматизация документооборота, внедрение систем видеонаблюдения, аналитических платформ и инструментов искусственного интеллекта для выявления и оценки коррупционных рисков. Использование этих решений способствует ускорению обработки информации, повышению объективности контроля и укреплению общественного доверия к правоохранительной системе.

Важным направлением цифровизации правоохранительной деятельности является создание Единой системы видеомониторинга (ЕСВМ). Основной задачей ЕСВМ является объединение городских камер видеонаблюдения на единой платформе для формирования видеоаналитики в режиме реального времени. Система позволяет осуществлять распознавание лиц, анализировать поведенческие модели, выявлять оставленные предметы, задымление, возгорания и иные события, требующие оперативного реагирования [2].

Существенную роль в предупреждении коррупционных правонарушений играют персональные видеорегистраторы (видеожетоны), используемые сотрудниками патрульной полиции. Постоянная видеофиксация служебной деятельности способствует повышению уровня подотчетности сотрудников и обеспечивает объективную доказательственную базу при рассмотрении жалоб граждан. 30 апреля 2025 года Министерством внутренних дел Республики Казахстан утверждены нормы снабжения сотрудников полиции видеожетонами, предусматривающие обязательное оснащение сотрудников патрульной полиции средствами видеофиксации [3].

Следует отметить, что применение технологий видеоаналитики способствует реализации принципа неотвратимости контроля. Осознание факта постоянного видеонаблюдения оказывает превентивное воздействие на сотрудников органов внутренних дел, снижая вероятность совершения коррупционных правонарушений. Кроме того, автоматизированный анализ видеоданных позволяет своевременно выявлять нарушения служебной дисциплины и признаки коррупционного поведения без непосредственного вмешательства человека.

Несмотря на положительные результаты внедрения систем видеонаблюдения, видеожетонов и интеллектуальных платформ видеоаналитики, их функциональные возможности в настоящее время используются преимущественно для фиксации уже совершенных событий и последующего анализа полученной информации. Такой подход обеспечивает контроль и документирование нарушений, однако не позволяет в полной мере осуществлять комплексное прогнозирование коррупционных рисков и предупреждать противоправное поведение сотрудников органов внутренних дел. В связи с этим представляется актуальным переход к новым моделям цифрового контроля, основанным на технологиях искусственного интеллекта и предиктивной аналитики.

В этой связи представляется целесообразным создание в системе Министерства внутренних дел Республики Казахстан единой интеллектуальной платформы антикоррупционного видеоанализа, функционирующей на основе технологий искусственного интеллекта и машинного обучения. Основной задачей такой системы должно стать выявление коррупциогенных ситуаций на ранних стадиях и автоматическое информирование подразделений собственной безопасности о возможных нарушениях антикоррупционного законодательства и служебной дисциплины.

Предлагаемая система может быть интегрирована с действующими средствами видеонаблюдения, персональными видеожетонами сотрудников полиции, системами контроля доступа, служебными информационными базами и

цифровыми платформами МВД. Это позволит осуществлять комплексный мониторинг служебной деятельности сотрудников в режиме реального времени.

В частности, система сможет автоматически фиксировать случаи необоснованного отключения видеожетонов или прекращения видеозаписи в период исполнения служебных обязанностей. Подобные факты могут свидетельствовать о попытках скрыть противоправные действия либо избежать последующего контроля со стороны руководства [4].

Дополнительным направлением работы системы может стать анализ служебных маршрутов сотрудников. На основании данных геолокации и информации о служебных заданиях искусственный интеллект сможет выявлять необоснованные отклонения от маршрута патрулирования, посещение объектов, не связанных с исполнением служебных обязанностей, а также нахождение сотрудников в неустановленных местах в рабочее время без соответствующего разрешения руководства.

Особый интерес представляет возможность выявления неформальных контактов сотрудников полиции с лицами, ранее привлекавшимися к уголовной ответственности либо состоящими на профилактических учетах. При систематическом выявлении подобных контактов вне рамок процессуальной деятельности система может автоматически формировать уведомления для подразделений собственной безопасности с целью проведения дополнительной проверки.

Важным элементом интеллектуального контроля может стать мониторинг соблюдения порядка приема граждан. Искусственный интеллект способен фиксировать случаи проведения встреч без обязательной регистрации, отсутствие видеофиксации предусмотренных процедур, а также нарушения установленных регламентов взаимодействия сотрудников полиции с населением.

Перспективным направлением является внедрение технологии поведенческой видеоаналитики. На основе анализа больших массивов данных система сможет выявлять нетипичные модели поведения сотрудников, которые статистически связаны с повышенным риском коррупционных правонарушений. Например, частое отключение средств видеофиксации, регулярное пребывание в определенных местах вне служебной необходимости, многократные контакты с одними и теми же лицами, а также иные отклонения от стандартных алгоритмов служебной деятельности.

Принципиальным преимуществом предлагаемой системы является переход от реагирования на уже совершенные коррупционные правонарушения к их предупреждению. В отличие от традиционных методов контроля, основанных на последующем анализе информации, интеллектуальная видеоаналитика позволит выявлять потенциальные коррупционные риски еще до наступления негативных последствий.

Внедрение такой системы будет способствовать повышению прозрачности деятельности органов внутренних дел, укреплению служебной дисциплины, снижению уровня латентной коррупции и повышению доверия граждан к правоохранительным органам. Кроме того, использование технологий искусственного интеллекта позволит существенно снизить нагрузку на

подразделения собственной безопасности за счет автоматизации процессов мониторинга и выявления коррупционных рисков.

Практическая реализация подобных решений требует не только совершенствования технической инфраструктуры органов внутренних дел, но и модернизации системы профессиональной подготовки кадров. Будущие сотрудники органов внутренних дел должны обладать знаниями в области цифровой криминалистики, искусственного интеллекта, анализа данных, информационной безопасности и применения интеллектуальных систем контроля в правоохранительной деятельности. В этой связи представляется целесообразным включение в образовательные программы ведомственных учебных заведений дисциплин, посвященных использованию технологий видеоаналитики, цифровому мониторингу служебной деятельности и применению искусственного интеллекта в предупреждении коррупции.

Кроме того, внедрение интеллектуальных систем видеоаналитики будет способствовать формированию у будущих сотрудников органов внутренних дел устойчивой антикоррупционной культуры, основанной на принципах открытости, подотчетности и неотвратимости контроля. Осознание возможностей современных цифровых технологий и механизмов объективного контроля должно стать важным элементом профессионального правосознания сотрудников правоохранительных органов.

Таким образом, интеллектуальные системы видеоаналитики следует рассматривать не только как инструмент предупреждения коррупционных правонарушений в органах внутренних дел, но и как важное направление совершенствования профессиональной подготовки кадров для правоохранительной системы. Переход от модели фиксации уже совершенных нарушений к модели прогнозирования и предупреждения коррупционных рисков требует подготовки специалистов нового поколения, способных эффективно использовать возможности цифровых технологий в интересах обеспечения законности и правопорядка.

Список литературы:

1. Указ Президента Республики Казахстан Касым-Жомарта Токаева № 1151 от 6 января 2026 года 2026 г. Об объявлении Года цифровизации и искусственного интеллекта // https://adilet.zan.kz/rus/docs/U2600001151

2. Концепция развития органов внутренних дел Республики Казахстан на 2023-2027 годы. – Астана, 2023 // https://www.gov.kz/memleket/entities/qriim/documents/details/402466?lang=ru

3. Об утверждении норм снабжения сотрудников органов внутренних дел техническими средствами видеофиксации: приказ МВД Республики Казахстан от 30 апреля 2025 года // https://adilet.zan.kz/rus/docs/G25C0000349

4. МВД развивает цифровизацию полицейской деятельности// https://www.gov.kz/memleket/entities/qriim/press/news/details/501969?lang=ru&utm_source=chatgpt.com

БУЗАКАНОВА АЙЖАН БАХИТХАНОВНА
Старший преподаватель кафедры общеюридических дисциплин
Костанайской академии МВД Республики Казахстан
имени Ш.Кабылбаева
магистр права

ФОРМИРОВАНИЕ КУЛЬТУРЫ ОТВЕТСТВЕННОГО ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ОБУЧАЮЩИМИСЯ: ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ

Стремительное развитие технологий искусственного интеллекта является одной из наиболее заметных характеристик современной цифровой трансформации общества. Генеративные системы искусственного интеллекта получили широкое распространение и используются для поиска и обработки информации, подготовки текстов, анализа данных, перевода, создания изображений, программирования и решения образовательных задач. В связи с этим образовательные организации сталкиваются не столько с вопросом о том, следует ли разрешать использование искусственного интеллекта, сколько с необходимостью определить, как сформировать у обучающихся культуру его безопасного, законного, этичного и ответственного применения.

Актуальность данной проблемы для системы высшего образования Республики Казахстан существенно возросла в связи с формированием специального правового регулирования искусственного интеллекта. 17 ноября 2025 года был принят Закон Республики Казахстан № 230-VIII ЗРК «Об искусственном интеллекте». [1].

Принятие специального закона свидетельствует о переходе от преимущественно технологического восприятия искусственного интеллекта к его рассмотрению как объекта правового регулирования. Для образовательной сферы это означает необходимость формирования у обучающихся представлений не только о возможностях ИИ, но и о связанных с ним правовых обязанностях, рисках и принципах ответственного поведения.

Особенно значима данная проблема для высших учебных заведений Министерства внутренних дел Республики Казахстан. Будущий сотрудник органов внутренних дел будет осуществлять профессиональную деятельность в условиях цифровизации государственного управления, правоохранительной деятельности и информационного пространства. Поэтому культура использования искусственного интеллекта должна формироваться уже в период обучения.

Культура ответственного использования искусственного интеллекта представляет собой совокупность знаний, навыков, ценностей и моделей поведения человека, обеспечивающих законное, безопасное, этичное и осознанное применение ИИ-технологий.

В отличие от обычной цифровой грамотности, которая предполагает способность пользоваться информационными системами и цифровыми ресурсами, культура ответственного использования ИИ включает более широкий круг компетенций.

Во-первых, обучающийся должен понимать возможности и ограничения искусственного интеллекта. ИИ способен быстро обрабатывать значительные объемы информации и генерировать связный текст, однако результат его работы не обязательно является достоверным.

Во-вторых, необходима информационная критичность. Обучающийся должен уметь проверять полученную информацию по надежным источникам.

В-третьих, важна правовая грамотность. Использование ИИ не должно нарушать законодательство Республики Казахстан.

В-четвертых, необходима этическая ответственность. Пользователь должен понимать последствия передачи информации ИИ, особенности авторства, недопустимость дискриминационного использования технологий и необходимость человеческого контроля.

Исследователи E. Kasneci и соавторы отмечают, что внедрение больших языковых моделей в образование требует формирования у преподавателей и обучающихся специальных компетенций, позволяющих понимать ограничения таких систем, проверять факты и критически оценивать результаты их работы [4].

Таким образом, основная задача современного образования заключается не в том, чтобы научить обучающегося просто пользоваться ChatGPT или другой ИИ-системой. Значительно важнее научить его правильно принимать решения при использовании искусственного интеллекта**.**

Формирование культуры ответственного использования ИИ невозможно без знания обучающимися нормативных требований.

Ключевое значение имеет Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК [1]. Закон устанавливает правовые основы использования технологий искусственного интеллекта и закрепляет основные понятия, связанные с данной сферой.

Для образовательного процесса это означает, что обучающиеся должны постепенно знакомиться с основными правовыми принципами использования ИИ.

Особое значение имеет понимание того, что искусственный интеллект не освобождает человека от ответственности за совершенные действия. Использование цифрового инструмента само по себе не является основанием для освобождения от соблюдения закона.

Вторая важнейшая группа правовых отношений связана с персональными данными.

Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» регулирует отношения, связанные со сбором, обработкой и защитой персональных данных [2]. Данное положение имеет непосредственное отношение к использованию генеративных ИИ-систем.

Например, обучающийся может захотеть получить от ИИ анализ конкретной ситуации и загрузить в систему текст заявления, характеристики, протокола, анкеты или другого документа. Если такой документ содержит персональные данные, его передача стороннему сервису может создать правовые и информационные риски.

Поэтому одним из базовых правил цифровой культуры должно стать следующее:

Не следует передавать в публичные ИИ-системы персональные данные и иную информацию ограниченного доступа без соответствующего правового основания и разрешенных условий обработки.

Для курсантов вузов МВД это правило приобретает особое значение, поскольку будущая профессиональная деятельность будет связана с информацией, имеющей повышенную чувствительность.

Правового регулирования недостаточно для формирования ответственного поведения. Даже если определенное действие прямо не запрещено законодательством, оно может быть этически проблемным.

В образовательной среде прежде всего необходимо обратить внимание на четыре этических принципа:

Первый принцип — честность. Обучающийся должен понимать разницу между использованием ИИ как вспомогательного инструмента и передачей искусственному интеллекту выполнения всей учебной работы.

Например, использование ИИ для поиска идей или объяснения сложного понятия может способствовать обучению. Однако представление полностью сгенерированного текста в качестве самостоятельно выполненной работы ставит под сомнение академическую добросовестность.

Второй принцип — прозрачность. В случаях, когда правила образовательной организации предусматривают раскрытие факта использования ИИ, обучающийся должен указывать, каким образом технология была использована. Например: «При подготовке работы использовалась система генеративного искусственного интеллекта для предварительной структуризации материала. Все нормативные положения и фактические сведения проверены автором по официальным источникам». Подобный подход формирует ответственное отношение к технологии.

Третий принцип — критичность. ИИ не должен восприниматься как абсолютный источник истины. Языковая модель может создать текст, который выглядит научным и убедительным, но содержит ошибочные сведения. В исследовании Kasneci и соавторов отдельно подчеркиваются риски неточности, предвзятости результатов и необходимость постоянного человеческого контроля [4].

Четвертый принцип — безопасность. Обучающийся должен учитывать, какие сведения он передает ИИ-системе, где они могут обрабатываться и какие последствия может иметь их раскрытие.

UNESCO в своем руководстве по генеративному ИИ в образовании и исследованиях делает акцент на человекоцентричном подходе, защите конфиденциальности данных, этическом использовании технологий и необходимости формирования соответствующих компетенций [3].

Одной из наиболее дискуссионных проблем является использование ИИ при написании учебных и научных работ. Распространение генеративных моделей существенно изменило традиционное понимание самостоятельной работы. Ранее преподаватель мог предположить, что текст курсовой работы создан непосредственно обучающимся. Сегодня технически возможно за несколько минут получить связный текст практически на любую тему.

Однако наличие текста еще не означает наличие знаний. Именно поэтому традиционные формы контроля нуждаются в определенной трансформации. Например, вместо того чтобы оценивать исключительно письменный реферат, преподаватель может попросить обучающегося:

- объяснить основные положения работы;
- обосновать выбор источников;
- назвать использованные нормативные акты;
- указать слабые стороны сформулированной позиции;
- привести практический пример;
- защитить собственный вывод.

Такая форма контроля позволяет определить, действительно ли обучающийся понимает содержание работы. Исследование Meyer и соавторов также обращает внимание на вопросы справедливого использования больших языковых моделей, их потенциальной предвзятости и необходимости осторожного отношения к точности генерируемых результатов [5].

Таким образом, искусственный интеллект требует не отмены академических требований, а их адаптации к новой технологической среде.

Особое значение рассматриваемая проблема приобретает при подготовке курсантов высших учебных заведений МВД.

Курсант должен понимать, что цифровая грамотность сотрудника органов внутренних дел включает не только умение пользоваться информационными системами. Она предполагает ответственное обращение с информацией, понимание рисков цифровых технологий и соблюдение правовых требований.

В профессиональной деятельности сотрудник может столкнуться с персональными данными граждан, материалами проверок, процессуальными документами, служебной информацией и цифровыми доказательствами.

Поэтому навыки, сформированные во время обучения, непосредственно влияют на будущую профессиональную деятельность.

Представляется целесообразным включить в образовательный процесс специальный модуль:

«Правовые и этические основы использования искусственного интеллекта».

Такой модуль может включать следующие темы:

1. Понятие и виды искусственного интеллекта.
2. Законодательство Республики Казахстан об искусственном интеллекте.
3. Защита персональных данных при использовании ИИ.
4. Академическая добросовестность и генеративный ИИ.
5. Проверка достоверности информации.
6. Алгоритмическая предвзятость.
7. Ответственность человека при использовании ИИ.
8. Информационная безопасность.
9. Этические стандарты применения ИИ.
10. Практические кейсы из деятельности органов внутренних дел.

Особенно эффективным может стать кейс-метод. Например, курсанту предлагается следующая ситуация. Курсант получил задание подготовить

аналитическую справку. Для ускорения работы он загрузил в открытый ИИ-сервис документ, содержащий сведения о гражданине и обстоятельства конкретного правонарушения.

ИИ сформировал аналитический текст.

Перед обучающимся ставятся вопросы:

1. Какие сведения были переданы ИИ?
2. Содержат ли они персональные данные?
3. Какие правовые риски возникли?
4. Можно ли использовать полученный результат?
5. Какие действия должен был совершить курсант?
6. Как изменить алгоритм работы, чтобы исключить нарушение требований безопасности?

Такой кейс одновременно формирует правовую, цифровую и этическую компетентность.

Одним из центральных принципов ответственного использования ИИ должен стать human oversight — человеческий контроль**.**

В образовательной практике это означает, что окончательное решение всегда должно оставаться за человеком. UNESCO рассматривает использование генеративного ИИ в образовании именно в рамках человекоцентричного подхода и обращает внимание на необходимость обеспечения безопасного, этичного и содержательного использования технологии [3].

Для будущего сотрудника правоохранительных органов этот принцип имеет особую значимость. Нельзя представить ситуацию, при которой сотрудник говорит: «Такой вывод сделал искусственный интеллект, поэтому я не несу за него ответственности». Подобная логика несовместима с профессиональной деятельностью сотрудника ОВД. ИИ может быть инструментом анализа, но не субъектом профессиональной ответственности. Поэтому уже в процессе обучения необходимо формировать установку:«ИИ помогает принять решение, но не принимает решение вместо профессионала».

Для формирования культуры ответственного использования ИИ у обучающихся целесообразно реализовать комплекс мероприятий.

Во-первых, необходимо разработать внутренние правила использования ИИ в образовательном процессе**.**

В них можно определить разрешенные и запрещенные формы применения ИИ.

Во-вторых, следует включать вопросы цифровой этики в содержание юридических дисциплин.

Например, при изучении конституционного права можно обсуждать защиту прав человека в условиях алгоритмического управления; при изучении административного права – использование автоматизированных систем государственными органами; при изучении уголовного права – вопросы цифровых доказательств и рисков автоматизированной оценки; при изучении информационного права – обработку персональных данных.

В-третьих, необходимо развивать навыки фактчекинга.

Любая юридически значимая информация, полученная от ИИ, должна проверяться по официальным источникам.

В-четвертых, следует обучать работе с нормативными правовыми актами.

Курсант должен понимать, что ИИ не заменяет обращение к официальной базе законодательства.

В-пятых, необходимо развивать у обучающихся понимание этических последствий использования технологий.

Таким образом, ответственное использование ИИ должно стать не отдельным факультативным навыком, а частью общей культуры будущего специалиста.

Искусственный интеллект постепенно становится неотъемлемой частью образовательной и профессиональной среды. Его использование предоставляет обучающимся значительные возможности для поиска, анализа и систематизации информации, однако одновременно создает новые правовые, этические и информационные риски.

В Республике Казахстан формирование правовой культуры использования ИИ получает особое значение в связи с принятием Закона «Об искусственном интеллекте» [1]. Одновременно требования законодательства о защите персональных данных устанавливают важные ограничения при обработке информации посредством цифровых систем [2].

Для образовательных организаций это означает необходимость перехода от простой модели «разрешить или запретить ИИ» к более содержательной модели формирования культуры ответственного использования технологии.

Такая культура должна включать пять взаимосвязанных элементов:

правовая грамотность – информационная критичность – этическая ответственность – цифровая безопасность – человеческий контроль.

Для курсантов высших учебных заведений МВД данные элементы приобретают особое значение, поскольку в будущем они будут работать с информацией, непосредственно связанной с обеспечением правопорядка и защитой прав граждан.

Следовательно, задача современного ведомственного образования заключается не в полном исключении искусственного интеллекта из образовательного процесса, а в формировании у курсантов способности использовать его законно, критически, безопасно и этично**.**

В конечном итоге ответственное использование ИИ должно рассматриваться как один из элементов современной профессиональной и правовой культуры обучающегося.

Список литературы:

1. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК.

2. О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 года № 94-V.

3. Miao F., Holmes W. *Guidance for Generative AI in Education and Research*. Paris: UNESCO, 2023. / https://ifap.ru/library/book670.pdf

4. Kasneci E., Sessler K., Küchemann S. et al. ChatGPT for good? On opportunities and challenges of large language models for education // *Learning and Individual Differences*. 2023. Vol. 103. Article 102274. DOI: 10.1016/j.lindif.2023.102274.

5. Meyer J. G., Urbanowicz R. J., Martin P. C. N. et al. ChatGPT and large language models in academia: opportunities and challenges // *BioData Mining*. 2023. Vol. 16. Article 20. DOI: 10.1186/s13040-023-00339-9.

6. Об образовании: Закон Республики Казахстан от 27 июля 2007 года № 319-III.

ГАЛИЕВ СЕРИК ЖАКИПБЕКОВИЧ
кандидат юридических наук, доцент,
Заслуженный работник МВД РК

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ В СОВРЕМЕННЫЙ ПЕРИОД: РОЛЬ ТЕОРИИ ОРД

Тема настоящей конференции является исключительно актуальной и позвольте поблагодарить организаторов за возможность принять участие в ее работе.

Цифровая трансформация всех сфер казахстанского общества стала реальностью наших дней и данный процесс неуклонно набирает все более растущую силу. Под этот объективный, отвечающий велениям времени процесс, проведены крупные государственные меры, создано новое министерство, приняты соответствующие правовые документы и т.д. 2026 год в Казахстане объявлен Годом цифровизации и искусственного интеллекта. Глава государства во всех Посланиях народу Казахстана, в других своих выступлениях неоднократно высказывался по этой проблеме, разъясняя и нацеливая всех на необходимость своевременной и адекватной реакции на глобальные вызовы. Так, выступая в январе текущего года на V Национальном Курултае в Кызыл-Орде Президент Республики Казахстан подчеркнул: «Казахстан вступил на путь форсированного развития цифровизации и внедрения искусственного интеллекта во все сферы общественной и личной жизни. … Успешными станут нации, сумевшие адаптироваться к новой реальности, созданной искусственным интеллектом, и, более того, активно, предметно участвующие в процессе формирования такой реальности».

Все это исключительно актуально и для сферы правопорядка и такого специфического ее направления как оперативно-розыскная деятельность (ОРД).

В настоящее время цифровая трансформация в области ОРД безусловно должна стать стратегическим направлением деятельности оперативных подразделений государственных органов – субъектов ОРД. С появлением и все более быстрым развитием современных информационных технологий многие преступления совершаются уже в виртуальном пространстве. Криминальные структуры все более активно осваивают новое поле преступной деятельности. Об этом свидетельствуют не только официальная уголовная статистика, но и средства массовой информации. Редко, когда в ежедневных новостных лентах ТВ и радио не упоминается о преступлениях, совершаемых с использованием искусственного интеллекта и других современных технологий. Наносимый ущерб только физическим лицам исчисляется уже в миллионах тенге.

Криминализация социальных сетей, мессенджеров, средств электронных платежей, сети Интернет стала очевидным явлением. Поток заявлений граждан, пострадавших от такого рода преступлений не иссякает, а постоянно нарастает. Противоправная активность в цифровой среде вызывается и тем, что она сама по своей природе способствует сохранению преступникам анонимности, что безусловно оказывает негативное влияние на принцип неотвратимости наказания. И

здесь роль оперативно-розыскной деятельности просто нельзя переоценить. Аксиомой звучит выражение: «Тайные способы совершения преступлений требуют и тайных способов борьбы с ними».

Нужно четко осознавать, что ответственная задача по опережению замыслов и действий преступников, вычислению их самих и их намерений, принятию мер по предотвращению преступлений и умению застигать преступников на месте преступления не может быть решена без всемерного укрепления и развития оперативно-розыскной функции уголовной юстиции.

Действующий закон Республики Казахстан «Об оперативно-розыскной деятельности» в числе основных задач предписывает выявление преступлений, что ориентирует оперативные аппараты на сбор информации, носящей преимущественно скрытый характер, о действиях преступников, внешне ведущих законопослушный образ жизни. Всем присутствующим известно, что экономические, финансовые, коррупционные и большинство уголовных тяжких преступлений, совершаемых в условиях неочевидности, выявляются и раскрываются большей частью именно оперативны путем.

По самой своей природе оперативно-розыскная деятельность, имеет ярко выраженный поисковый характер, в следствие чего выполняет важную роль не только на различных этапах уголовного судопроизводства, но и активно осуществляется до стадии досудебного расследования. Роль и значение потенциала оперативно-розыскных возможностей в проверочных мероприятиях как после официальной регистрации сообщения о преступлении, так и до получения такового, трудно переоценить.

Оперативно-розыскная деятельность является наиболее эффективным инструментом изучения противоправной среды, где большинство процессов протекает скрытно, с использованием многочисленных приемов маскировки, различных ухищрений и конспирации. Это подтверждается и бесспорно доказывается всей многовековой историей человеческой цивилизации.

Однако казахстанские реалии выглядят несколько иначе. Поясним эту мысль подробнее.

Почему в основополагающем документе, определяющим стратегические направления развития правовой системы Республики Казахстан и вектор ее развития на десять лет вперед даже не упоминается, вопреки действующему законодательству, о такой важнейшей функции борьбы с преступностью, как оперативно-розыскная деятельность? Речь идет о Концепции правовой политики Республики Казахстан на период до 2030 года (1). Между тем в двух предыдущих аналогичных правовых актах оперативно-розыскной деятельности, как функции уголовной юстиции, уделялось должное внимание.

Так, в первой Концепции правовой политики Республики Казахстан до 2010 года (2), наряду с гуманизацией уголовной политики указывалось на объективную необходимость ужесточения ее в отношении лиц, виновных в совершении тяжких и особо тяжких преступлений, скрывающихся от уголовного преследования, а также при рецидиве преступлений, а это, как известно, невозможно без совершенствования оперативно-розыскных мер. Далее в документе прямо констатировалось: «Приоритетными направлениями должны стать

предупреждение и профилактика преступности, наступательность в борьбе с нею, совершенствование оперативно-розыскной деятельности, адекватное реагирование на реально складывающуюся оперативную обстановку, повышение уровня информационного обеспечения и аналитической работы». Концепция нацеливала на то, что «особое значение будет уделено своевременному введению норм, направленных на предупреждение и пресечение распространения наркомании и наркобизнеса, терроризма, этнического и религиозного экстремизма, торговли людьми, особенно женщинами и детьми, компьютерной преступности, незаконного изготовления и оборота огнестрельного оружия, его частей, компонентов и боеприпасов к нему, международных преступлений коррупционного характера, а также относящихся к сфере «отмывания» денег». Нет смысла убеждать и доказывать, что в этой многогранной и трудоемкой работе приоритетную роль играет оперативно-розыскная деятельность правоохранительных органов и спецслужб любого государства.

В Концепции правовой политики Республики Казахстан на период с 2010 до 2020гг. (3), указывалось, что «требуется разработка оптимальных правовых механизмов, предусматривающих эффективное применение уголовно-процессуального законодательства и законодательства об оперативно-розыскной деятельности» (п.2.9.). Важной задачей соответствующих структур государства ставилась «неукоснительное соблюдение законности, прав и свобод граждан при осуществлении оперативно-розыскной деятельности. В этом плане необходимо усиливать систему гарантий прав и свобод граждан, обеспечивать неприкосновенность частной жизни, ответственность за незаконное использование средств и методов оперативно-розыскной деятельности».

Отмеченное принижение, если не сказать сильнее, оперативно-розыскной деятельности, наблюдаемое на протяжении многих лет, является, к сожалению, далеко не единичным фактом. Коренные изменения в уголовном судопроизводстве Казахстана, происходившие в первые десятилетия нового века, неоднозначно воспринимались в среде оперативных, следственных и прокурорских работников. В это время активно высказывались мнения, что сфера оперативно-розыскной деятельности должна быть резко сужена, что данная государственно-правовая форма борьбы с преступностью себя изживает. Зазвучали голоса о ненужности ОРД и даже постановки Закона Республики Казахстан «Об оперативно-розыскной деятельности» на утрату. Новый импульс такие суждения получили в связи с тем, что 12 оперативно-розыскных мероприятий (ОРМ) вошли в Главу 31 «Негласные следственные действия» нового уголовно-процессуального кодекса (УПК) РК. Но ни в коем случае нельзя сводить всю оперативно-розыскную деятельность только к оперативно-розыскным мероприятиям, при всей их значимости. Недопустимо, чтобы целое поглощалось, хотя и безусловно важным, но все же его частью.

Примечательны в этом плане и результаты проведенных научных изучений проблемы. К примеру, в одном из исследований, осуществленном нами еще более десяти лет назад было опрошено 94 оперативных работников, в том числе выдвинутых в резерв на замещение руководителей оперативных подразделений органов ведущих борьбу с экономической и коррупционной преступностью. На вопрос: «Считаете ли Вы оперативную работу актуальной в настоящее время?» 78%

ответили положительно, 5% считают, что можно обойтись без нее, 6 % полагают, что специальные ОРМ могут вполне ее заменить, 9% затруднились с ответом и 2% обошли молчанием этот вопрос. Как видим даже в среде сотрудников, которые непосредственно осуществляют оперативно-розыскную работу, нет полного единства в ее действенности и нужности. Такое положение явно недопустимо.

Хотя пик огульного охаивания оперативно-розыскной деятельности как якобы аморального инструментария уголовной юстиции вплоть до попыток отождествления ее с практикой политических репрессий и других нарушений законности [4, с. 12–13] остался позади, но, как видим, рецидивы такого мышления сохраняются и по настоящее время, подпитываясь односторонним, непрофессиональным (а зачастую и предвзятым) восприятием практики, теории и правового регулирования ОРД. Заметим, что попытки объявить оперативно-розыскную деятельность чуть ли не анахронизмом, и, как минимум принизить ее значимость в противодействии преступности, не прекращались и в момент подготовки проекта Концепции правовой политики Республики Казахстан на 2021-2030 годы, что и отразилось на ее содержании.

В этом же ряду и следующие обстоятельства.

Первое – Закон Республики Казахстан «Об оперативно-розыскной деятельности» был принят 15 сентября 1994 года. С того времени прошло ровно 32 года в течение которых в него вносились изменения и дополнения, связанные преимущественно, с проводимой в стране судебно-правовой реформой. Этому вопросу мы посвящали специальные публикации (5). К настоящему времени закон сильно устарел и совершенно не отражает сегодняшние правовые, экономические, социальные и научно-технические реалии. Однако коренная переработка этого основополагающего для правоохранительных органов и спецслужб законодательного акта длительное время тормозилась. Только по истечении 30 лет со дня ввода в действие закона была создана межведомственная рабочая группа, которой удалось подготовить сильныйьзаконопроект, практически отвечающий реалиям времени, но внесение его в Парламент страны затягивается.

Второе. За 32 года действия этого основополагающего для борьбы с преступностью закона был подготовлен лишь один Комментарий к нему (6). Хотя тираж той работы по нынешним временам был рекордным – пять тысяч экземпляров, он разошелся быстро, что свидетельствовало о его большой востребованности как практиками, так и учеными. Через несколько лет ко мне лично обращались руководители оперативных подразделений и их сотрудники с настоятельной просьбой помочь им приобрести указанный Комментарий, вплоть до его ксерокопирования. Прошло уже почти три десятилетия, но ученые в области ОРД продолжают молчать, тогда как практики, слушатели и курсанты учебных заведений силовых структур, студенты гражданских юридических вузов остро нуждаются в такой работе.

Кстати, это яркий пример состояния оперативно-розыскной науки Казахстана. Ведь для того, чтобы прокомментировать доступным для понимания рядовым оперативным работником норм законодательства, ориентирующим его повседневную деятельность по противодействию криминалу, от ученого требуется

не только солидный теоретический уровень, но и хорошее знание практики борьбы с преступностью и, желательно, личный практический опыт в этой сфере.

Если мы поставим вопрос: готова ли на сегодня оперативно-розыскная наука предложить практике готовые рецепты использования искусственного интеллекта при проведении отдельных оперативно-розыскных мероприятий или же документирования выявленных преступных действий? Скорее всего с большей вероятностью ответ будет отрицательным.

Самый совершенный уголовный закон во многих случаях может оказаться бессильным без разработки надлежащего инструментария его реализации. Важной составляющей такого правового механизма является оперативно-розыскная деятельность соответствующих государственных органов. Идти вперед только эмпирическим путем, силами практиков – субъектов ОРД, путем проб и ошибок – непозволительная роскошь в наше динамичное время. Не заниматься серьезно теорией все равно, что без карты идти по незнакомой местности. Именно она, теория, должна освещать путь практике – **это аксиома**. Не требует доказательств положение, что научные результаты теории ОРД существенно обогащают и повышают потенциал борьбы с преступностью, поднимают эту борьбу на качественно иной, более высокий уровень.

Назрела необходимость создания единого научно-исследовательского центра, который будет разрабатывать тематику актуальных научных исследований, контролировать их проведение и отдачу, организовывать публикацию научных работ преимущественно с закрытым грифом и защиту диссертаций, выращивать научные кадры, готовить замену уходящих ученым и т.д. В начале 2000-х годов в МВД РК был создан научно-исследовательский институт, но хорошую и нужную идею без должной подготовки и организационного обеспечения тогдашнее руководство министерства провалило. Отсутствие научной глубины и трезвого расчета на перспективу развития, недостаточный, мягко говоря, учет кадровых, материальных и финансовых ресурсов, поспешность, если не сказать суетливость при решении организационных вопросов, стремление быстрее «отчитаться» закономерно привели к скорому и бесславному закрытию института. Что стало с судьбами сотрудников НИИ, их человеческими надеждами на обустройство в новой столице, на перспективу научного и профессионального роста – можно и не говорить.

Учитывая этот негативный опыт, но понимая исключительную необходимость концентрации научных исследований в области ОРД в «одних руках», вносим предложение создать при Академии управления МВД РК научно-исследовательскую лабораторию по указанному научному профилю. Только лишь разработка научной тематики в едином центре автоматически приведет к устранению разнобоя, мелкотемья и упорядочения научных исследованиий, организационно их направит, позволит четче видеть и корректировать перспективу развития теории ОРД. Для примера – посмотрите тематику докторских и магистерских диссертаций во всех вузах МВД. Бросается в глаза явный крен в сторону дисциплин уголовного права, уголовно-исполнительного права, криминологии, уголовного процесса... Проблемы оперативно-розыскной деятельности исследуются совершенно недостаточно, тогда как именно в них

наиболее остро нуждается практика борьбы с преступностью. Отдельная и очень актуальная проблема – внедрение результатов научных исследований в области ОРД в практику органов внутренних дел, авторское и академическое их сопровождение.

По мере укрепления лаборатории, подготовки специалистов уголовно-криминалистического блока, расширения научных исследований, усиления их значимости и отдачи для практики и подготовки кадров, повышения авторитета в научных кругах и практических органов можно приступить к проработке реорганизации ее в научно-исследовательский институт. Главное не оказаться на обочине научно-технического прогресса, не отстать от впереди идущих, не оказаться в положении вечно догоняющих.

Глобальная цифровая цивилизация не дает времени на привычную раскачку и затягивание назревших вопросов. Ведомственная наука должна на систематической основе осмысливать складывающуюся в стране криминогенную ситуацию и адекватно ей вырабатывать соответствующие проекты решений, выдавать научно обоснованные предложения, рекомендации и алгоритмы, разрабатываемые по запросам практических подразделений на основе обобщения и систематизации передового опыта практики деятельности оперативных подразделений полиции, что возможно только при упорядочении научных исследований.

Необходимо приступить к скорейшей разработке Стратегии внедрения информационных технологий в оперативно-розыскную деятельность, что значительно ускорит становление теории ОРД в Казахстане и задаст четкий вектор ее развития. Проблемы эти носят универсальный характер и мало зависят от ведомственной принадлежности оперативно-розыскного органа. Они касаются всех аспектов противодействия преступности и угроз национальной безопасности.

Еще на рубеже 1960-1970-х годов основоположники теории ОРД в трудных теоретических дебатах последовательно и убедительно доказали самостоятельность теории ОРД как отрасли научного знания и сформулировали предмет ее познания. Сегодня объектом внимания оперативно-розыскной науки должны стать и вопросы противоправного поведения в киберпространстве и противодействия ему, включая возможности искусственного интеллекта. Оперативно-розыскная наука призвана вырабатывать теоретическую модель цифровых технологий, разрабатывать прикладные технологические решения для оперативных подразделений субъектов ОРД, а это – наукоемкий процесс, требующий глубокого и сложного научного обоснования и без развития соответствующей теории здесь не обойтись. Нужна консолидация усилий ученых всех субъектов ОРД для развития в стране единой оперативно-розыскной теории. Предпосылки для этого имеются.

Обеспечить в области правопорядка гарантированные в новой Конституции страны (7) права и свободы человека и гражданина невозможно без применения специфического инструментария ОРД и развития ее теории.

Закончить выступление хотелось бы цитатой из трудов одного из основоположников рассматриваемой отрасли научного знания, которая актуально звучит и сегодня: «Теоретическое осмысливание ОРД – единственная возможность обеспечить не интуитивное, а преимущественно научно обоснованное и поэтому

более успешное применение соответствующих средств и методов при решении практических задач» (8, с. 27).

Список литературы:

1. Концепция правовой политики Республики Казахстан на период до 2030года. Утверждена Указом Президента Республики Казахстан от 15 октября 2021 года № 674.

2. Концепция правовой политики Республики Казахстан до 2010 года. Одобрена Указом Президента страны № 949 от 20 сентября 2002 года.

3. Концепция правовой политики Республики Казахстан на период с 2010 до 2020гг. Утверждена Указом Президента Республики Казахстан от 24 августа 2009 года № 858.

4. Галиев С.Ж. Оперативно-розыскная деятельность органов финансовой полиции. Общая часть. Учебное пособие. – Астана, 2006. – 218 С.

5. Галиев С.Ж. К характеристике оперативно-розыскного закона. «Профилактическая деятельность государства как одно из средств сдерживания преступности». Матер.научн.-практ.конф. – Алматы, Акад. МВД РК, 2006. 0,5 п.л.; Галиев С.Ж. Динамика взгляда законодателя на оперативно-розыскной закон Казахстана. Научные труды Академии финансовой полиции. Выпуск 7. Астана, 2006. 0,6п.л.

6. Галиев С.Ж., Сапарин О.Е. Комментарий к Закону Республики Казахстан «Об оперативно-розыскной деятельности». -Алматы, изд. «Жеті жарғы», 1998.

7. Конституция Республики Казахстан. Принята на республиканском референдуме 15 марта 2026 года.

8. Гребельский Д.В. Теоретические основы и организационно-правовые проблемы оперативно-розыскной деятельности органов внутренних дел: Монография.-М., Академия МВД СССР, 1977.

ГЛУБОКОВСКИХ РОМАН ВЛАДИМИРОВИЧ
Доцент кафедры оперативно-розыскной деятельности
органов внутренних дел Калининградского филиала
Санкт-Петербургского университета МВД России
кандидат юридических наук, полковник полиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОПЕРАТИВНО-РОЗЫСКНОМ ПРОГНОЗИРОВАНИИ: ПРАВОВЫЕ, ОРГАНИЗАЦИОННЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ

Современные вызовы, стоящие перед розыскными подразделениями уголовного розыска, требуют перехода от реактивных к проактивным методам работы. Рост количества лиц, объявляемых в федеральный и межгосударственный розыск, увеличение мобильности скрывающихся преступников, использование ими цифровых технологий для сокрытия данных о своей личности формируют устойчивый запрос на научно обоснованные, верифицируемые методы прогнозирования поведения скрывшихся преступников, перемещения без вести пропавших лиц и идентификации неопознанных трупов.

Как справедливо отмечает М.Э. Джафарова, «применение ИИ в ОРД регулируется федеральными законами, включая № 144-ФЗ[1] и № 149-ФЗ[2], а судебная практика подтверждает его допустимость при условии соблюдения прав граждан»[1]. Однако автор выделяет ряд существующих проблем: «необходимость баланса между автоматизацией и человеческим контролем, риски нарушения конфиденциальности данных, этические вопросы и неполноту существующего правового регулирования»[1]. Особую актуальность данная проблематика приобретает в свете того, что преступники уже активно используют технологии ИИ в противоправных целях.

Цель настоящей статьи – на основе эмпирических данных выявить актуальные проблемы внедрения технологий искусственного интеллекта в оперативно-розыскное прогнозирование и предложить направления их решения.

Эмпирическую базу исследования составили анкетирование 270 сотрудников оперативных, следственных и информационно-аналитических подразделений органов внутренних дел (150 сотрудников розыска, 70 следователей, 50 аналитиков); анализ 500 материалов по розыску лиц различных категорий граждан за период 2001–2026 годов из различных региональных розыскных подразделений уголовного розыска; интервьюирование экспертов в сфере розыскной работы (руководители подразделений, наиболее опытные оперативники, аналитики, преподаватели ведомственных вузов); личный опыт автора по установлению местонахождения (задержанию) лиц, скрывшихся от органов дознания, следствия и суда.

[1] Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 01.04.2025) "Об оперативно-розыскной деятельности"

[2][2] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 26.06.2026) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2026).

В настоящее время в правоохранительных органах Российской Федерации активно внедряются следующие технологии на базе искусственного интеллекта:

1. Биометрическая идентификация и распознавание лиц. Системы «Сфера» и NtechLab активно используются для идентификации подозреваемых.
2. Анализ больших данных (Big Data). Технологии предиктивной аналитики применяются для обнаружения интересующих фактов, прогнозирования преступности и разработки превентивных мер. Как подчеркивается в научной литературе, «внедрение систем, способных анализировать большие объемы данных для выявления связей и закономерностей в деятельности преступных групп» является перспективным направлением[2].
3. Нейросети для анализа серийных преступлений. МВД России внедряет специализированные нейросети для составления цифровых портретов правонарушителей. На основе собранных на месте преступления доказательств нейросеть прогнозирует дальнейшие действия злоумышленников и сужает круг поиска[3].
4. Система «Зеркало», позволяющая нейросетям составлять психологические профили подозреваемых на основе анализа их поведения, коммуникаций и иных цифровых следов. Рассмотрено возможное применение НС «Зеркало» для МВД с целью выявления кибермошенничества[4].
5. Выявление дипфейков. Министерство тестирует программы на основе ИИ для выявления поддельных фото-, видео- и аудиоматериалов, что особенно актуально в свете участившихся случаев использования дипфейков для совершения мошенничеств[6].

Правовое регулирование применения ИИ в ОРД осуществляется в рамках Указа Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») и Указа Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Применение ИИ в оперативно-розыскной деятельности регулируется также федеральными законами, включая № 144-ФЗ «Об оперативно-розыскной деятельности» и № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Проведенное исследование выявило существенный разрыв между декларируемой цифровизацией оперативно-розыскной деятельности и реальным положением дел.

Результаты анкетирования 270 респондентов выявили, что 80% оперуполномоченных и 64% следователей формируют прогнозы преимущественно на основе личного опыта и профессиональной интуиции. Лишь 3% сотрудников розыска и 7% следователей используют формализованные методики и алгоритмы. Специализированное программное обеспечение для прогнозирования не применяет никто (0% во всех группах). Низкий уровень знакомства с передовыми технологиями подтверждается тем, что 40% оперуполномоченных и 40% следователей не знакомы с технологиями Big Data и искусственного интеллекта. Еще 50% в каждой группе «слышали о них, но подробно не изучали». Лишь 10% хорошо знакомы с потенциальными преимуществами этих технологий. Вопросы

кадрового дефицита высвечиваются через ответы 67% оперативных сотрудников, которые ощущают «острую потребность» в получении дополнительных знаний и навыков в области аналитической работы и прогнозирования. Еще 30% считают полезным прохождение курсов повышения квалификации. В информационном обеспечении, ни один из респондентов не считает существующие информационные системы полностью обеспечивающими прогностические потребности. 50% сотрудников розыска констатируют, что системы обеспечивают лишь «в незначительной степени». 60% оперуполномоченных и 50% следователей оценивают межведомственный обмен информацией как неудовлетворительный. Высокий запрос на цифровизацию акцентируют 80% сотрудников розыска и 90% аналитиков, которые убеждены, что внедрение формализованных прогностических моделей значительно повысит эффективность розыскной работы.

Анализ 500 материалов в отношении разыскиваемых лиц, различных категорий за 2001–2026 годы подтвердил системные проблемы:

1. Только в 23% случаях зафиксированы целенаправленные попытки применения прогнозного анализа. В 77% материалов работа велась по шаблону, без прогноза и его анализа.
2. В 87% материалов отсутствует систематическая работа по проверке и уточнению выдвинутых прогностических версий (принцип верифицируемости не соблюдается).
3. Лишь в 6% материалов план оперативно-розыскных мероприятий был конкретным и логически вытекал из прогностических версий. При этом в 93% этих случаев (28 из 30 материалов) розыск завершился успешно.
4. В 90% материалов, где розыск не увенчался успехом, методы прогнозирования не применялись.
5. Средний срок успешного розыска с применением прогнозирования составил 22 дня, без него - 78 дней (сокращение в 3,5 раза).

Результаты исследования указывают на наличие прямой зависимости между прогностическим подходом и эффективностью розыска. Однако существующая практика строится преимущественно на интуитивно-эмпирическом уровне, формализованные методики и специализированное программное обеспечение фактически не применяются. Это создает «окно возможностей» для внедрения технологий искусственного интеллекта и машинного обучения в прогностическую деятельность.

Анализ научной литературы и правоприменительной практики позволяет выделить следующие ключевые правовые проблемы внедрения ИИ в ОРД, это:

1. Неполнота правового регулирования. Как обоснованно отмечается в литературе, «применение ИИ в ОРД регулируется федеральными законами, включая № 144-ФЗ и № 149-ФЗ, а судебная практика подтверждает его допустимость при условии соблюдения прав граждан. Однако автор выделяет ряд существующих проблем: необходимость баланса между автоматизацией и человеческим контролем, риски нарушения конфиденциальности данных, этические вопросы и неполноту существующего правового регулирования»[1].
2. Отсутствие легального определения правового статуса ИИ. В законодательстве не закреплено, является ли ИИ субъектом, объектом или

инструментом оперативно-розыскной деятельности. Как отмечают исследователи, «предлагается внесение изменений в уголовно-процессуальное законодательство РФ, направленных на четкое определение правового статуса ИИ, обеспечение прозрачности алгоритмов, защиту персональных данных и усиление судебного контроля»[1].

3. Проблема допустимости доказательств. Как справедливо указывает О.В. Тепляков, «между моментом получения этой информации оперативными подразделениями и моментом ее представления в суде в качестве полноценного доказательства лежит глубокая правовая и методологическая пропасть»[6]. Применение ИИ для генерации прогностических выводов ставит вопрос: можно ли использовать результаты машинного анализа в качестве доказательств, и если да – то при каких условиях?

Основными организационными проблемами внедрения искусственного интеллекта в прогнозную деятельность розыскных подразделений уголовного розыска мы считаем следующие:

1. Как показало исследование, для обеспечения деятельности по прогнозированию при формировании документов стратегического планирования необходимы специалисты с соответствующим образованием, позволяющим с технической точки зрения осуществлять прогнозирование, а также обладающие знаниями и опытом в области борьбы с преступностью. «Сейчас в этой сфере наблюдается пробел»[7].

2. Отсутствие единой цифровой платформы. Как отмечается в научной литературе, перспективным направлением является создание единой цифровой платформы прогнозирования в рамках федеральной информационной системы стратегического планирования (в соответствии со ст. 14 Федерального закона от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации»).

3. Проблемы межведомственного взаимодействия. (60% оперуполномоченных и 50% следователей оценивают межведомственный обмен информацией как неудовлетворительный, отмечая длительные бюрократические задержки и неполноту получаемой информации)

Внедрение искусственного интеллекта в оперативно-розыскную деятельность поднимает серьезные этические вопросы, требующие осмысления, к таковым можно отнести:

1. Риск усиления социальных предубеждений. Главная проблема – риск усиления социальных предубеждений через алгоритмы, обученные на нерепрезентативных данных. Алгоритмы машинного обучения, построенные на исторических данных о преступности, могут воспроизводить и усиливать существующие системные искажения. Как отмечают исследователи, «ключевыми угрозами являются отсутствие всеобъемлющего законодательства, проблемы прозрачности алгоритмов, риски нарушений прав человека, алгоритмическая предвзятость и проблема ответственности за решения, принятые на основе ИИ»[1].

2. Одной из ключевых этических проблем является непрозрачность алгоритмов ИИ (проблема «черного ящика»). Граждане, в отношении которых принимаются решения на основе прогнозов ИИ, имеют право знать, на основании

каких критериев эти решения приняты. Это особенно актуально, когда речь идет о мерах процессуального принуждения.

3. Широкое применение технологий ИИ в правоохранительной деятельности сопряжено с рисками нарушения конфиденциальности данных.

4. Как справедливо подчеркивается в научной литературе, «особое значение придается тому, что ИИ должен оставаться вспомогательным инструментом, а окончательные решения должны принимать уполномоченные люди»[1]. Роль искусственного интеллекта должна всегда оставаться вспомогательной и не подменять собой познавательную деятельность человека.

5. На международном уровне также уделяется внимание этическим аспектам применения ИИ в правоохранительной деятельности. Страны БРИКС одобрили декларацию, подчеркивающую важность соблюдения этических стандартов при использовании технологий – обеспечение уважения человеческого достоинства, предотвращение предвзятости и дискриминации, противодействие дезинформации и создание соответствующих механизмов надзора. Европол опубликовал рамочный документ по этическим технологиям в правоохранительной деятельности[8; 9].

На основе проведенного исследования предлагаются следующие направления совершенствования:

В части правового регулирования предлагается:

- внесение изменений в Федеральный закон № 144-ФЗ «Об оперативно-розыскной деятельности» с целью закрепления возможности использования технологий искусственного интеллекта и машинного обучения для решения задач оперативно-розыскной деятельности;
- разработка и принятие ведомственного нормативного акта, регламентирующего порядок применения прогностических алгоритмов, включая требования к их научной обоснованности, верифицируемости, понятности и контролируемости;
- законодательное закрепление требований к прозрачности алгоритмов ИИ, используемых в правоохранительных целях, с обеспечением права граждан на обжалование решений, принятых на основе автоматизированных прогностических систем;
- определение правового статуса результатов, полученных с помощью технологий ИИ, и порядка их трансформации в уголовно-процессуальные доказательства.

В организационном аспекте:

- выделение в системе МВД России из числа существующих аналитических подразделений) сотрудников для осуществления прогностической деятельности с использованием технологий ИИ;
- разработка и внедрение автоматизированных информационно-аналитических систем с модульной структурой, интегрированных с существующими базами данных и оперативными учетами (АДИС «Папилон», ФР-«Оповещение», ФР-«Опознание», ПТК «Розыск-Магистраль»);

- формирование единой межведомственной прогностической платформы, обеспечивающей доступ к данным ФНС, ФССП, УВМ, ПФР, кредитно-финансовых учреждений для целей прогнозирования;

- применение геоинформационных систем (ГИС) для пространственного анализа розыскной ситуации и визуализации прогностических данных.

В подготовке кадров для оперативных подразделений считаем необходимым включение в образовательные программы ведомственных вузов специальных тем по оперативно-розыскной прогностике с применением технологий OSINT и GEOINT, а также создание тренажерных комплексов для отработки навыков работы с прогностическим программным обеспечением.

Проведенное исследование позволяет сформулировать следующие выводы:

1. Оперативно-розыскное прогнозирование является неотъемлемым и научно обоснованным элементом современной оперативно-розыскной деятельности. Его внедрение позволяет существенно сократить время на розыск скрывшихся лиц (в 3,5 раза), оптимизировать расход оперативно-розыскных ресурсов и усилить профилактическую составляющую работы уголовного розыска.
2. Существующая практика прогнозирования в розыскной работе носит преимущественно интуитивно-эмпирический характер. 80% сотрудников полагаются на личный опыт и интуицию, формализованные методики и специализированное ПО фактически не применяются. Это создает объективную необходимость внедрения технологий искусственного интеллекта и машинного обучения.
3. Внедрение ИИ в ОРД сдерживается комплексом правовых, организационных и этических проблем: неполнота правового регулирования, отсутствие легального определения статуса ИИ, кадровый дефицит, отсутствие специализированного ПО, риски нарушения конфиденциальности, алгоритмической предвзятости и размывания ответственности.
4. Грамотное регулирование ИИ в ОРД позволит повысить эффективность борьбы с преступностью, сохранив при этом права граждан и принципы верховенства права.
5. Ключевым принципом внедрения ИИ должно оставаться его использование в качестве вспомогательного инструмента при сохранении окончательного контроля за человеком.

Перспективы развития оперативно-розыскного прогнозирования неразрывно связаны с его цифровизацией – внедрением технологий искусственного интеллекта для анализа больших данных, созданием интеллектуальных систем поддержки принятия решений и развитием соответствующей правовой базы, обеспечивающей как эффективность, так и законность этой деятельности. Только симбиоз высококвалифицированных кадров, продуманной правовой основы и передовых технологий позволит оперативно-розыскному прогнозированию раскрыть свой полный потенциал в деле повышения эффективности розыскной работы.

Список литературы:

1. Джафарова, М. Э. Искусственный интеллект в оперативно-розыскной деятельности: его роль, применение и правовой статус / М. Э. Джафарова // Новый юридический журнал. – 2025. – № 3. – С. 39-45.

2. Кубасов, И. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России / И. А. Кубасов, Л. А. Лекарь // Труды Академии управления МВД России. – 2023. – № 3(67). – С. 154-161.

3. Жданов, Ю.Н. Полиция будущего / Ю.Н. Жданов, В.С. Овчинский. – Москва : [б. и.], 2018. – 165 с.

4. Смирнов, С. В. Применение нейронных сетей в России / С. В. Смирнов // Информационные технологии в решении задач инновационного развития : Сборник статей международной научной конференции, Сыктывкар, 15 декабря 2023 года. – Санкт-Петербург: Гуманитарный национальный исследовательский институт НАЦРАЗВИТИЕ, 2023. – С. 35-39.

5. В МВД тестируют новые программы для выявления дипфейков // https://www.vedomosti.ru/society/articles/2026/07/01/1210179-mvd-testiruet-ii-dlya-viyavleniya-dipfeikov. 2026. 1 июля.

6. Тепляков, О. В. Проблемы взаимной оценки доказательств и оперативно-розыскной информации / О. В. Тепляков // Тенденции развития оперативно-розыскной деятельности : Сборник материалов межведомственного круглого стола, посвященного памяти доктора юридических наук А.М. Ефремова, Иркутск, 24 октября 2025 года. – Иркутск: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Восточно-Сибирский институт Министерства внутренних дел Российской Федерации», 2025. – С. 59-63.

7. Глубоковских Р. В. Оперативно-розыскное прогнозирование в розыскной работе подразделений уголовного розыска : монография. Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2026 – 133с.

8. БРИКС [Электронный ресурс] // РИА Новости. – с 2025. – URL: https://ria.ru/20250707/briks-2027573942.html?ysclid=mtk9zdjwl5800276 (дата обращения: 25.08.2026).

9. Готоцев П. М., Душкин Р. В., Кузнецов О. П., Мильке В. Э., Незнамов А. В., Потапова Е. Г. Этичное применение искусственного интеллекта // Этика в эпоху цифровых технологий. – Раздел 3.3. – [Электронный ресурс]. – URL: https://ethics.cdto.ranepa.ru/3_3?ysclid=mtka7ab0m869025929 (дата обращения: 25.08.2026)

ГРИНЕВА ДАРЬЯ АЛЕКСЕЕВНА
Начальник кафедры оперативно-розыскной деятельности
органов внутренних дел Калининградского филиала
Санкт-Петербургского университета МВД России
кандидат юридических наук, полковник полиции

СИСТЕМА УЧЕТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ: ПРОБЛЕМЫ И ПУТИ СОВЕРШЕНСТВОВАНИЯ

Несмотря на очевидные достижения, современная система учетов органов внутренних дел (далее ОВД) сталкивается с рядом проблем, снижающих эффективность информационного обеспечения оперативных подразделений.

Анализ научных публикаций [1; 2; 3] и практического опыта автора позволяет выделить следующие актуальные проблемы формирования, ведения и использования учетов:

1) Неоднородность и фрагментированность информационных систем. Исторически различные виды учетов создавались обособленно, на разных технологических платформах. Например, дактилоскопическая база АДИС, базы розыска транспортных средств, «Портрет» (фотоучет) и другие длительное время существовали разрозненно, что создавало трудности при их интеграции. Например, происходило дублирование данных либо отсутствовало централизованное объединение [4]. Несмотря на создание ИБД-Ф, до настоящего времени не все локальные учеты полностью синхронизированы. Уровень технической оснащенности в регионах различается, в ряде субъектов сохраняются устаревшие программные продукты.

2) Неполнота и устаревание данных. Полнота учета зависит от своевременного и тщательного внесения сведений. На практике имеют место упущения: не все объекты ставятся на учет надлежащим образом. Например, некоторые регионы могут не направлять в ГИАЦ информацию о преступлениях небольшой тяжести, вследствие чего федеральная база остается неполной. Либо задержанного дактилоскопировали, но из-за технического сбоя данные не поступили в центральную базу. В результате проверки по учету могут не дать результата, хотя соответствующая информация существует на локальном уровне. Устаревание данных проявляется в том, что по истечении срока давности или при наступлении иных обстоятельств информация должна сниматься с учета, однако не всегда это происходит своевременно и влечет загромождение системы неактуальными данными.

3) Проблемы достоверности и качества информации. При ручном вводе данных возможны ошибки (опечатки в фамилиях, неверные даты и прочее). Так, при объединении баз выявлялись случаи, когда одно и то же лицо значилось под разными учетными записями (например, из-за разночтения фамилии), либо, наоборот, разные лица объединялись в одну запись.

4) Ограниченный доступ и режим секретности. Принцип конспиративности учетов безусловно важен, однако, избыточная секретность порой препятствует обмену информацией. Например, данные оперативного учета могут иметь гриф

секретности либо являться «для служебного пользования», и ряду сотрудников, которым эти сведения могли бы оперативно помочь, не доступны. Баланс между защитой информации и ее доступностью не всегда соблюдается оптимально. Имеют место случаи, когда территориальные подразделения неохотно делятся информацией с коллегами, особенно если сведения добыты оперативным путем и представляют ценность для раскрытия серии преступлений (вследствие наличия конкуренции между подразделениями и отражением в последующем результата в статистической отчетности) [5].

5) Юридические ограничения использования учетных данных. Несмотря на высокую практическую ценность оперативных учетов, их результаты не всегда могут непосредственно использоваться в суде в качестве доказательств. Например, установление личности по дактилоскопическому учету является оперативной информацией и для придания ей доказательственного значения необходимо проведение судебной экспертизы. Аналогичным образом сведения о предыдущих судимостях обвиняемого, полученные из справки информационного центра, могут оцениваться судом лишь при вынесении приговора, но не как доказательство его вины в конкретном преступлении.

6) Технические и кадровые проблемы. Поддержание значительных массивов данных требует современной техники и квалифицированных ИТ-специалистов. Не во всех территориальных ОВД имеется достаточное количество компьютерной техники, сканеров, а также доступ к защищенным каналам связи. Обновление программного обеспечения представляет собой отдельную проблему (зачастую устаревает и не поддерживается разработчиком). Кадровый аспект выражается в том, что сотрудники информационных и экспертно-криминалистических центров не всегда успевают обработать поток данных, вследствие чего возникают задержки при постановке на учет [6].

Исходя из указанных проблем, можно предложить следующие пути совершенствования системы учетов в оперативной деятельности ОВД:

1. Дальнейшая интеграция и централизация учетов. Необходимо завершить создание единой информационной платформы МВД, в рамках которой все ключевые учеты (оперативно-справочные, розыскные, криминалистические) будут связаны и доступны через единый интерфейс. Проект интегрированной базы данных (10-14 основных учетов, доступных во всех ОВД) уже провозглашен, и следует ускорить его реализацию.

2. Автоматизация и использование современных технологий. Внедрение технологий больших данных (Big Data) и искусственного интеллекта способно существенно повысить эффективность учетов. Например, методы машинного обучения могут применяться для выявления скрытых связей между объектами в учетах (криминальный анализ больших данных). Биометрические технологии позволяют автоматически распознавать лица на фотографиях и видео и сопоставлять их с фотоучетами (подобные системы уже используются в городах Москва и Санкт-Петербург, будучи интегрированными с базами МВД). В геномных учетах целесообразно применение высокопроизводительных алгоритмов для быстрого сравнения ДНК-профилей. Перспективным направлением представляется также применение технологий искусственного интеллекта для интеллектуального

анализа данных уголовной регистрации. В частности, алгоритмы машинного обучения могут использоваться для выявления неочевидных связей между событиями и лицами, прогнозирования серийности преступлений, автоматического выявления аномалий в учетных данных. Обработка естественного языка позволяет автоматизировать анализ текстовой информации (протоколов, рапортов, ориентировок) и извлекать из нее сведения, подлежащие постановке на учет. Системы компьютерного зрения обеспечивают распознавание лиц, автомобильных номеров, объектов на изображениях и видеозаписях, их автоматическое сопоставление с массивами фото- и видеоучетов. Голосовые биометрические системы позволяют идентифицировать личность по образцам речи, что особенно актуально при раскрытии преступлений, совершенных с использованием средств связи. Кроме того, применение искусственного интеллекта способно снизить нагрузку на сотрудников за счет автоматизации рутинных операций по вводу, сверке и систематизации данных, минимизировать влияние человеческого фактора на качество учетной информации. Следует отметить, что внедрение таких технологий требует решения сопутствующих правовых и этических вопросов, включая обеспечение защиты персональных данных и недопущение дискриминационных алгоритмов, однако их потенциал для совершенствования системы учетов очевиден.

3. Обеспечение полноты и актуальности сведений. Для этого следует усилить контрольные механизмы: ввести автоматические напоминания и блокировки, например, при раскрытии дела – следователь незамедлительно направляет отметку для снятия преступления с учета как раскрытого; при освобождении лица – ФСИН направляет соответствующие данные в МВД. Возможно, целесообразно законодательно закрепить обязанность определенных органов предоставлять информацию в учеты МВД. Необходимо регулярно проводить актуализацию баз данных, выявлять и удалять устаревшие или ошибочные записи.

4. Повышение достоверности данных, внедрение стандартов качества. Предлагается внедрить единые стандарты оформления учетных документов (что уже частично сделано) и проводить обучение персонала правильному заполнению. Следует использовать справочники и автоматические проверки при вводе данных в электронные системы (например, система должна уведомлять о невозможности ввести несуществующую дату или допустить ошибку в номере паспорта).

5. Совершенствование правового регулирования использования информации. В частности, целесообразно рассмотреть вопрос о внесении изменений в Уголовно-процессуальный кодекс относительно статуса результатов оперативных учетов. Некоторые специалисты предлагают законодательно признать результаты криминалистических учетов (например, установление личности по отпечаткам) в качестве основания для возбуждения уголовного дела. В настоящее время зачастую требуется проведение повторной экспертизы с теми же данными, что затягивает процесс. Если дактилоскопическая база дала однозначное совпадение, возможно допустить использование заключения специалиста в качестве доказательства без дублирования его экспертизой.

6. Усиление защиты информации при расширении доступа. Для повышения эффективности необходимо одновременно облегчить доступ добросовестным

пользователям и усилить защиту от утечек, посредствам внедрения дифференцированных систем доступа (каждый пользователь получает доступ строго к тем данным, которые необходимы ему по должности), а также технических средств защиты (шифрование каналов связи, двухфакторная аутентификация при доступе к базам).

7. Обучение и повышение квалификации сотрудников. Необходимо регулярно обучать оперативных работников и следователей возможностям современных учетов, проводить практические занятия, издавать методические пособия по использованию каждой базы данных. Вновь назначаемые сотрудники должны быть ознакомлены с перечнем доступных баз данных, их функционалом и порядком направления запросов. Одновременно следует повышать уровень подготовки ИТ-специалистов МВД, чтобы они могли сопровождать сложные информационные системы, осуществлять консультирование, разрабатывать обновления и оперативно устранять сбои.

8. Развитие межведомственной интеграции. В перспективе следует стремиться к созданию межведомственного хранилища данных, в которое поступала бы информация не только от полиции, но и от смежных структур (в пределах, установленных законом). В настоящее время МВД интегрирует учеты с базами ГИБДД (учет транспортных средств), ФНС (персональные данные), Росфинмониторинга (подозрительные финансовые операции), Росреестр (об объектах недвижимости и правообладателях) и др. Дальнейшее развитие предполагает создание единого цифрового профиля правонарушителя, доступного всем правоохранительным органам [7].

Подводя итог, отметим, что совершенствование системы учетов представляет собой динамичный процесс, требующий комплексного подхода. Как справедливо отмечалось в литературе, развитие учетов должно идти параллельно с развитием преступности и методов борьбы с ней [8]. Новые вызовы (киберпреступность, транснациональная преступность) обусловливают появление новых видов учетов, например, таких как учет киберинцидентов, баз данных голосовых образцов [9]. При этом, активное внедрение технологий искусственного интеллекта в практику ведения учетов является одним из ключевых направлений модернизации информационного обеспечения органов внутренних дел. Законодателю и практикам необходимо своевременно реагировать на эти потребности, обновляя нормативную базу и внедряя достижения науки и техники, опираясь на статью 11 Федерального закона от 07.02.20211 № 3-ФЗ (в редакции от 04.08.2026) «О полиции»[3]. При условии реализации обозначенных мер можно ожидать, что информационная составляющая работы органов внутренних дел станет еще более эффективной, а учеты – действенным инструментом в деятельности оперативных подразделений.

Список литературы:

1. Самойлова, Ю. М. Использование информационных технологий при решении задач органов внутренних дел: тенденции и проблемы / Ю. М. Самойлова, А. О. Соборов // Проблемы информационного обеспечения расследования преступлений : Материалы Всероссийского научно-практического круглого стола, Луганск, 28 апреля 2025 года. – Луганск: Луганская академия Следственного комитета Российской Федерации, 2025. – С. 70-75.

[3] https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 20.08.2026)

2. Макеева, И. А. Использование современных технологий и информационных систем сотрудниками органов внутренних дел / И. А. Макеева // Образование и право. – 2025. – № 10. – С. 692-694.

3. Симоненко, Е. И. Криминалистические учеты: современное состояние и перспективы развития / Е. И. Симоненко, А. М. Кушхов // Белгородские криминалистические чтения : Сборник научных трудов, Белгород, 26 апреля 2025 года. Выпуск 11. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2025. – С. 118-124.

4. Гринева, Д. А. Роль информационных технологий в розыске без вести пропавших лиц / Д. А. Гринева // Использование современных информационных технологий в правоохранительной деятельности и актуальные проблемы информационной безопасности : Сборник материалов Всероссийской научно-практической конференции, Калининград, 02 марта 2005 года. – Калининград: Калининградский юридический институт МВД России, 2005. – С. 83-87.

5. Теория оперативно-розыскной деятельности / О. А. Вагин, К. К. Горяинов, А. В. Земскова [и др.]. – 5-е издание, исправленное и дополненное. – Москва : Инфра-М, 2025. – 795 с.

6. Савельева, М. В. Криминалистика / М. В. Савельева, А. Б. Смушкин. – Москва : Редакционно-изд. объединение «Новая юстиция», 2020. – 236 с.

7. Дунаев, С. А. Использование криминалистических и розыскных учетов в оперативно-розыскной деятельности: современное состояние, проблемы, пути решения / С. А. Дунаев // Вестник науки. – 2023. – Т. 1, № 11(68). – С. 683-688.

8. Тихонов, А. В. Некоторые проблемы совершенствования информационного обеспечения оперативных аппаратов ОВД / А. В. Тихонов // Вестник Московского университета МВД России. – 2010. – № 3. – С. 157-158.

9. Глубоковских, Р. В. Совершенствование оперативно-розыскной и следственной деятельности в сфере противодействия киберпреступности: по результатам экспертного опроса сотрудников правоохранительных органов / Р. В. Глубоковских, А. Г. Стороженко // XIV Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии» : Материалы международной научно-практической конференции, Калининград, 12 декабря 2025 года. – Калининград: Санкт-Петербургский университет МВД РФ, 2026. – С. 121-123.

ДЖИГИТОВА РАУШАН НУРБУЛАТОВНА
Қазақстан Республикасының ІІМ
М.Бөкенбаев атындағы Ақтөбе заң институтының
Жалпы заң пәндері кафедрасының аға оқытушысы
заң ғылымдарының магистрі, полиция подполковнигі

ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРҒА ҚАРСЫ ІС-ҚИМЫЛДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ: ТАРИХИ ДАМУЫ ЖӘНЕ ҚАЗАҚСТАН ТӘЖІРИБЕСІ

Аңдатпа: *Мақалада қылмыспен күрес және оның алдын алу саласындағы жасанды интеллект технологияларының қалыптасу тарихы мен қазіргі даму тенденциялары қарастырылады. Зерттеу тарихи-салыстырмалы және жүйелік талдау әдістеріне негізделген, бұл автоматтандырылған жүйелердің қарапайым мәліметтер базасынан бастап қазіргі терең оқыту алгоритмдеріне дейінгі эволюциясын кешенді түрде көрсетуге мүмкіндік береді. Автор жасанды интеллекттің құқық қорғау саласындағы эволюциясын кезең-кезеңмен талдап, заманауи Қазақстанның (мысалы, «Сергек» жүйесі мен цифрлық криминалистика) тәжірибесіне баға береді. Мақалада отандық және шетелдік тәжірибе салыстырмалы түрде қаралып, жасанды интеллект негізіндегі болжау алгоритмдерінің қылмыстың алдын алудағы тиімділігі мен шектеулері талданады. Сондай-ақ, жасанды интеллектті қолданудың құқықтық және этикалық мәселелері талқыланады, атап айтқанда алгоритмдік әділдік, жеке өмірге қол сұғылмаушылық құқығы және автоматтандырылған шешімдердің сот-тергеу қызметіндегі орны қарастырылады. Мақала соңында автор Қазақстанда жасанды интеллект технологияларын құқық қорғау қызметіне енгізудің құқықтық негіздерін жетілдіру бойынша практикалық ұсыныстар тұжырымдайды.*

Түйін сөздер: *жасанды интеллект, қылмыстық құқық бұзушылық, «Сергек», цифрлық криминалистика, болжау алгоритмдері, құқық қорғау органдары, болжамды полициялық қызмет (Predictive Policing), компьютерлік көру, табиғи тілді өңдеу, биометриялық сәйкестендіру, алгоритмдік әділдік, киберқылмыс, дербес деректерді қорғау, электрондық қылмыстық іс.*

1. Кіріспе

XXI ғасырдағы ғылыми-техникалық прогресс қылмыстың сипаты мен онымен күрес әдістерін түбегейлі өзгертті. Қазіргі таңда жасанды интеллект және үлкен деректер (Big Data) технологиялары құқық қорғау органдарының жедел-іздестіру және қылмыстың алдын алу қызметіндегі басты құралына айналуда [1]. Қазақстан Республикасы да бұл үдерістен тыс қалмай, «Цифрлық Қазақстан» мемлекеттік бағдарламасы аясында құқықтық жүйені автоматтандыруды белсенді жүргізіп келеді [2]. Алайда, бұл технологиялық деңгейге жетудің өзіндік тарихи жолы мен құқықтық негіздері бар.

Тақырыптың өзектілігі қылмыстың сандық ортаға көшуімен және дәстүрлі тергеу әдістерінің жаңа сын-қатерлерге толық жауап бере алмауымен түсіндіріледі.

Киберқылмыс, алаяқтықтың цифрлық түрлері, әлеуметтік желілер арқылы жасалатын құқық бұзушылықтар — мұның бәрі құқық қорғау органдарынан жедел әрі интеллектуалды талдау құралдарын қолдануды талап етеді. Осыған байланысты жасанды интеллект технологияларының пайда болу тарихын, олардың теориялық негіздерін және практикалық қолданылу тәжірибесін кешенді түрде зерттеу ғылыми әрі қолданбалы маңызға ие болып отыр.

Мәселенің теориялық маңыздылығы сонымен қатар құқықтық ғылымда «алгоритмдік басқару» (algorithmic governance) деген жаңа ұғымның қалыптасуымен де байланысты. Дәстүрлі құқықтық реттеу тетіктері адам факторына негізделсе, жасанды интеллект негізіндегі жүйелер шешім қабылдау процесіне автоматтандырылған компонентті енгізеді. Бұл, өз кезегінде, жауапкершілік, әділеттілік және заңдылық қағидаттарын жаңаша қарастыруды қажет етеді, сондықтан мақалада көтерілген мәселелер тек қолданбалы емес, сонымен қатар терең теориялық-құқықтық сипатқа да ие.

Зерттеудің мақсаты — құқық қорғау саласындағы жасанды интеллект технологияларының қалыптасу кезеңдерін жүйелі түрде сипаттау, олардың артықшылықтары мен қауіп-қатерлерін анықтау, сондай-ақ Қазақстан Республикасындағы қолданыстағы тәжірибеге ғылыми талдау жасау болып табылады. Мақаланың міндеттері: 1) жасанды интеллекттің құқық қорғау қызметіндегі тарихи эволюциясын кезеңдерге бөліп қарастыру; 2) Қазақстандағы нақты жүйелер мен бастамаларды сипаттау; 3) осы саладағы құқықтық реттеу мен этикалық мәселелерді анықтап, оларды шешудің мүмкін жолдарын ұсыну.

Зерттеу нысанын анықтауда автор құқық қорғау органдарының қылмыспен күрес қызметіндегі автоматтандырылған ақпараттық-талдамалық жүйелерді, ал зерттеу пәні ретінде осы жүйелердің қалыптасу заңдылықтарын және оларды құқықтық реттеудің отандық және шетелдік тәжірибесін таңдап алды. Зерттеу барысында тарихи-құқықтық, салыстырмалы-құқықтық және жүйелік-құрылымдық талдау әдістері қолданылды, бұл жасанды интеллект технологияларының дамуын кезеңдерге бөліп, әр кезеңнің құқықтық-институционалдық ерекшеліктерін ашуға мүмкіндік берді.

Мақаланың ғылыми жаңалығы отандық заң әдебиетінде жасанды интеллект технологияларының құқық қорғау қызметіндегі эволюциясын кезеңдік тәсіл негізінде жүйелі түрде сипаттауға, оны Қазақстанның нақты институционалдық тәжірибесімен (мысалы, «Сергек» жүйесі, электрондық қылмыстық іс жүргізу тетіктері) байланыстыруға ұмтылысында жатыр. Мақаланың практикалық маңыздылығы ұсынылған қорытындылар мен ұсыныстардың құқық қорғау органдарының цифрлық трансформация стратегияларын әзірлеу, сондай-ақ тиісті заңнамалық актілерді жетілдіру барысында қолданылуы мүмкін болуымен айқындалады.

2. Қылмыспен күрестегі жасанды интеллект технологияларының даму тарихы

Құқық қорғау саласында автоматтандырылған жүйелерді қолданудың эволюциясын төрт негізгі тарихи кезеңге бөліп қарастыруға болады:

1. Бастапқы кезең (1960-1980 жылдар): Бұл кезеңде алғашқы электронды есептеуіш машиналар (ЭЕМ) тек қылмыскерлер мен іздеудегі тұлғалардың

картотекаларын, статистикалық мәліметтерді сақтау үшін қарапайым мәліметтер базасы ретінде қолданылды. 1980-ші жылдары АҚШ пен Батыс Еуропада криминалистердің логикалық ережелеріне сүйенетін алғашқы «сарапшылық жүйелер» (Expert Systems) пайда болды [1].

2. Цифрлық профайлинг кезеңі (1990 жылдар): Компьютерлердің қуаты артып, күдіктілердің мінез-құлқын, қылмыс жасау қолтаңбасын (Modus Operandi) талдайтын автоматтандырылған профайлинг жүйелері дамыды. Алғашқы географиялық ақпараттық жүйелер (GIS) арқылы қылмыстың картасын құру басталды.

Осы кезеңде маңызды рөл атқарған тағы бір бағыт — деректер қорларының өзара байланысуы. Полиция, прокуратура және сот органдарының дербес жүргізетін тізілімдері біртіндеп біріктіріле бастады, бұл тергеушілерге бір ізденіс жүйесінен бірнеше дереккөзге қатынас жасауға мүмкіндік берді. Дегенмен, бұл кезеңдегі жүйелер әлі де негізінен ережеге негізделген (rule-based) болды, яғни олар алдын ала белгіленген логикалық шарттар бойынша ғана жұмыс істеді және өзін-өзі оқыту қабілетіне ие болмады.

3. Болжау алгоритмдерінің дәуірі (2000-2015 жылдар): АҚШ-та PredPol (Predictive Policing) бағдарламасының шығуы құқық қорғау саласында үлкен серпіліс әкелді [3]. Жүйе өткен жылдардағы қылмыс статистикасын талдап, келесі құқық бұзушылықтың қай уақытта және қай ауданда болуы мүмкендігін жоғары дәлдікпен болжай алды. Сонымен қатар, биометриялық сәйкестендіру (бет-әлпетті тану) жүйелері іске қосылды.

4. Заманауи кезең (2015 жылдан бүгінге дейін): Нейрожелілер мен терең оқыту (Deep Learning) технологияларының дамуы [4]. Жасанды интеллект тек статистикамен шектелмей, әлеуметтік желілердегі мәтіндерді, қаржылық транзакцияларды, киберкеңістіктегі заңсыз әрекеттерді секунд ішінде талдап, киберқылмыспен және ақшаны жылыстатумен (anti-money laundering) күрестің негізгі құралына айналды.

Осы кезеңнің ерекшелігі — табиғи тілді өңдеу (Natural Language Processing) технологияларының дамуы арқылы құқық қорғау органдары үлкен көлемдегі мәтіндік деректерді (жеделхаттар, әлеуметтік желі жазбалары, электрондық хат алмасулар) автоматты түрде талдап, экстремистік немесе қатер төндіретін контентті анықтай алатын болды. Сонымен қатар, компьютерлік көру технологиясы бейнебақылау камераларынан түсетін ағынды деректерді нақты уақыт режимінде өңдеп, күдікті іс-әрекеттерді (төбелес, ұрлық, апат) автоматты түрде тіркеуге мүмкіндік берді. Дүниежүзілік тәжірибеде мұндай жүйелердің тиімділігі жоғары болғанымен, олардың дәлдігі мен алгоритмдік әділдігі туралы пікірталастар да үдей түсті — атап айтқанда, АҚШ-тағы COMPAS бағдарламасының нәсілдік ұқсастыққа негізделген жанама дискриминация тудыруы осы мәселенің көрнекі мысалы болды [3].

3. Жасанды интеллектті қолданудағы Қазақстанның тәжірибесі

Қазақстан Республикасы құқық қорғау қызметін цифрландыруда Орталық Азия өңірі бойынша көшбасшы орында тұр. Оның жарқын мысалдары келесідей:

«Сергек» интеллектуалды бейнебақылау жүйесі: Бұл отандық жасанды интеллект элементтері бар кешенді жүйе. Ол тек жол қозғалысы ережелерін бұзуды

тіркеп қана қоймай, компьютерлік көру (Computer Vision) технологиясы арқылы қоғамдық орындардағы қауіпсіздікті қамтамасыз етеді [5]. Жүйе іздеуде жүрген автокөліктерді, күдікті тұлғаларды бет-әлпеті (Face Recognition) арқылы тауып, жедел басқару орталықтарына дабыл береді.

Электрондық қылмыстық іс (ЭҚІ): ҚР Қылмыстық-процестік кодексінің 41-1-бабына сәйкес, қылмыстық іс жүргізу электрондық форматта жүзеге асырылуы мүмкін [6]. Қазіргі таңда ЕРДБ (Единый реестр досудебных расследований) жүйесіне жасанды интеллект элементтерін енгізу арқылы қылмыстық істердің материалдарын автоматты түрде сараптау, заңнамалық қарама-қайшылықтарды анықтау жүзеге асырылуда.

Талдау және болжау жүйелері: ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитеті жасанды интеллект негізінде қылмыстық ахуалды болжаудың электронды карталарын қолданады. Бұл полиция нарядтарын қылмыс қаупі жоғары аймақтарға тиімді бөлуге мүмкіндік береді.

Цифрлық криминалистика құралдары: Қазақстандық құқық қорғау органдары мобильді құрылғылар мен компьютерлік жүйелерден дәлелдемелерді алу үшін арнайы бағдарламалық қамтамасыз етуді қолдана бастады. Мұндай құралдар зерттеу барысында үлкен көлемдегі цифрлық ізді (файлдар, хабарламалар, геолокациялық деректер) автоматты түрде сұрыптап, тергеушінің жұмысын жеделдетеді. Сонымен қатар, киберполиция бөлімшелері әлеуметтік желілердегі заңсыз контентті (алаяқтық жарнамалар, есірткі саудасына байланысты жарияланымдар) анықтайтын мониторингтік жүйелерді енгізуде.

Халықаралық ынтымақтастық: Қазақстан Интерполдың және басқа да халықаралық құқық қорғау платформаларының цифрлық дерекқорларына қолжетімділікті кеңейтіп, шекара маңы қылмыстарымен (контрабанда, адам саудасы, киберқаржылық алаяқтық) күресуде трансшекаралық деректер алмасу тетіктерін жетілдіруде. Бұл бағыт, әсіресе, жасанды интеллект негізіндегі бейнеаналитика мен биометриялық сәйкестендіру жүйелерін көрші мемлекеттердің тәжірибесімен үйлестіру қажеттілігін көрсетеді.

Жалпы алғанда, Қазақстандағы жасанды интеллект негізіндегі жүйелердің енгізілуі полицияның реактивті (болған оқиғаға жауап беру) моделінен проактивті (алдын алу) моделіне көшуіне ықпал етіп отыр. Дегенмен, бұл жүйелердің тиімділігі көбіне деректердің сапасына, инфрақұрылымның дайындығына және мамандардың біліктілігіне тікелей байланысты болып қалуда.

Сонымен қатар, елдегі ірі қалаларда «ақылды қала» (Smart City) тұжырымдамасы аясында жүзеге асырылып жатқан жобалар да қылмыстың алдын алу тетіктерімен тығыз байланысты. Көше жарықтандыруын, көлік ағынын және қоғамдық көлікті бақылайтын сенсорлық жүйелерден түсетін деректер құқық қорғау органдарының талдамалық платформаларымен біріктірілуде, бұл қалалық ортадағы қауіпсіздік жағдайын кешенді бағалауға мүмкіндік береді. Алайда мамандардың пікірінше, мұндай интеграцияның толыққанды жүзеге асуы үшін ведомствоаралық деректер алмасудың бірыңғай стандарттарын әзірлеу қажет, себебі қазіргі уақытта әртүрлі мемлекеттік органдардың ақпараттық жүйелері бір-бірімен толық үйлесімді жұмыс істей бермейді.

4. Құқықтық реттеу және этикалық мәселелер

Жасанды интеллектті қылмыстық процеске енгізу тек техникалық емес, сонымен қатар терең құқықтық мәселе. Осы тұста бірнеше өзекті мәселені атап өту қажет:

1. Адам құқықтарының қорғалуы: Бет-әлпетті тану және жеке деректерді өңдеу барысында ҚР Конституциясының 18-бабында бекітілген «әркімнің жеке өміріне қол сұғылмауына құқығы» сақталуы тиіс [7].

2. Алгоритмдік қателіктер: Жасанды интеллект қателесуі мүмкін (мысалы, адамды ұқсастығына қарай қате тану). Сондықтан, құқықтық тұрғыда жасанды интеллект шығарған шешім ешқашан түпкілікті үкім немесе айыптау негізі бола алмайды. Ол тек көмекші, ақпараттық құрал рөлін атқаруы тиіс. ҚР ҚПК 113-бабына сәйкес дәлелдемелерді бағалау тек адам (тергеуші немесе судья) тарапынан жасалады [6].

3. Халықаралық стандарттар: Еуропалық Одақтың қабылдаған «Жасанды интеллект туралы актісі» (EU AI Act) бойынша, құқық қорғау органдарында жасанды интеллектті қолдану «жоғары қауіпті» (High-Risk AI) санатқа жатқызылған [8]. Қазақстан заңнамасы да осы халықаралық стандарттарға сай жасанды интеллектті қолдану шекарасын нақты бекітетін арнайы заңнамалық актілерді қажет етеді.

4. Ашықтық және түсіндірме алу құқығы (Right to Explanation): Азаматтың өзіне қатысты автоматтандырылған жүйе шығарған қорытындымен танысу және оның негіздемесін түсінуге құқығы болуы тиіс. «Қара жәшік» (black box) деп аталатын күрделі нейрожелілік модельдердің шешім қабылдау логикасының түсініксіздігі — сот пен тергеу барысында дәлелдемелердің тексерілуін қиындататын маңызды кедергі болып саналады. Сондықтан алгоритмдік аудит пен түсіндірме жасай алатын жасанды интеллект (Explainable AI) тәсілдерін дамыту қажеттілігі туындайды.

5. Деректерді қорғау және киберқауіпсіздік: Жасанды интеллект жүйелерінің жұмысы үлкен көлемдегі жеке деректерді жинау мен өңдеуге негізделген, бұл өз кезегінде осы деректердің қауіпсіздігін қамтамасыз ету мәселесін көтереді. «Қазақстан Республикасының дербес деректер және оларды қорғау туралы» Заңының талаптарына сәйкес, құқық қорғау мақсатында жиналған биометриялық және өзге де сезімтал деректердің шектен тыс сақталуына, үшінші тұлғаларға берілуіне жол берілмеуі тиіс.

Жоғарыда аталған мәселелерді ескере отырып, шетелдік тәжірибеде (мысалы, Еуропалық Одақ пен Ұлыбританияда) қалыптасқан «адамның бақылауы» (human oversight) принципін ұстану маңызды. Бұл принцип бойынша жасанды интеллект жүйесі қанша дәрежеде дәл болса да, түпкілікті құқықтық маңызы бар шешімді әрдайым білікті маман қабылдауы тиіс, ал автоматтандырылған жүйе тек ақпараттық-талдамалық қолдау көрсету функциясын атқарады. Қазақстанда да осы принципті заңнамалық деңгейде бекіту, жасанды интеллект жүйелерін сертификаттау мен тәуелсіз аудиттен өткізу тетіктерін енгізу ұсынылады.

5. Қорытынды

Жасанды интеллекттің даму тарихы көрсеткендей, бұл технология құқық қорғау жүйесінің тиімділігін арттыруда таптырмас құрал. «Сергек» жүйесі мен цифрлық тергеу амалдары арқылы Қазақстан бұл бағытта үлкен жетістіктерге жетті.

Алайда, технологиялық прогресс заң үстемдігі мен адам құқықтарын шектемеуі тиіс.

Жүргізілген талдау негізінде келесі ұсыныстарды тұжырымдауға болады: біріншіден, құқық қорғау саласында қолданылатын жасанды интеллект жүйелерін міндетті түрде сертификаттаудан және тәуелсіз алгоритмдік аудиттен өткізу тетігін заңнамалық түрде бекіту қажет; екіншіден, жасанды интеллект негізіндегі шешімдердің адам құқықтарына ықпалын бағалайтын арнайы сараптама рәсімін енгізу тиімді болмақ; үшіншіден, тергеушілер мен сот қызметкерлерін жасанды интеллект технологияларының мүмкіндіктері мен шектеулерін түсінуге бағытталған біліктілікті арттыру бағдарламаларымен қамтамасыз ету қажет. Аталған шаралар Қазақстанда жасанды интеллект технологияларын құқық қорғау қызметіне енгізудің теориялық негіздемесі мен практикалық тетіктерін одан әрі жетілдіруге ықпал ететін болады.

Қорыта айтқанда, алдағы уақытта Қазақстанда құқық қорғау саласындағы жасанды интеллект алгоритмдерінің ашықтығы мен қауіпсіздігін реттейтін ұлттық құқықтық базаны одан әрі жетілдіру қажет. Тек осындай теңгерімді тәсіл ғана технологиялық инновацияны құқықтық мемлекет қағидаттарымен үйлестіруге мүмкіндік береді.

Әдебиеттер тізімі:

1. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

2. «Цифрлық Қазақстан» мемлекеттік бағдарламасын бекіту туралы. Қазақстан Республикасы Үкіметінің Қаулысы.

3. Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. NYU Press.

4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

5. «Сергек» зияткерлік жүйесі қоғамдық қауіпсіздікті қамтамасыз ету құралы ретінде. ҚР ІІМ ресми ақпараттық порталы.

6. Қазақстан Республикасының Қылмыстық-процестік кодексі. 2014 жылғы 4 шілдедегі № 231-V ҚРЗ.

7. Қазақстан Республикасының Конституциясы (2026 жылғы 15 наурызда республикалық референдумда қабылданып, 2026 жылғы 1 шілдеден бастап қолданысқа енген жаңа редакциясы).

8. European Parliament. (2024). Artificial Intelligence Act (EU AI Act). Официальный текст Регламента Европейского Союза.

ДЮСЕБЕКОВА САБИНА БУЛАТОВНА
Докторант 2 курса Академии управления
МВД Республики Казахстан
магистр права

ЦИФРОВОЕ ПОВЕДЕНИЕ СОТРУДНИКА ПОЛИЦИИ КАК ФАКТОР ПРОФЕССИОНАЛЬНОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *В статье исследуется цифровое поведение сотрудника полиции как фактор профессиональной безопасности в условиях внедрения искусственного интеллекта в деятельность правоохранительных органов. Обосновывается, что расширение применения технологий искусственного интеллекта в деятельности органов внутренних дел увеличивает значение человеческого фактора. Показано, что сведения, размещаемые сотрудником в цифровой среде, могут становиться объектом автоматизированного анализа, использоваться для формирования цифрового профиля и в дальнейшем применяться для социальной инженерии, фишинга, дискредитации либо подготовки противоправных действий. Предлагается рассматривать цифровое поведение не только как элемент служебной этики и информационной культуры, но и как самостоятельный криминологически значимый фактор профессиональной безопасности сотрудника полиции. Сформулированы предложения по совершенствованию нормативного и организационного регулирования цифрового поведения сотрудников органов внутренних дел Республики Казахстан.*

Ключевые слова: *искусственный интеллект, цифровое поведение, сотрудник полиции, профессиональная безопасность, информационная безопасность, цифровая гигиена, цифровой след, персональные данные, правоохранительная деятельность.*

Введение

«Каждое наше цифровое решение – это не просто технология, а инструмент реализации главного принципа «Закона и порядка», – отметил министр внутренних дел Республики Казахстан Саденов Е.С. По его словам, цифровая экосистема Министерства внутренних дел становится неотъемлемой частью национальной безопасности [1].

Данное положение важно для понимания изменений, которые происходят в деятельности органов внутренних дел. Цифровизация правоохранительной деятельности меняет не только технические возможности полиции, но и сам характер работы сотрудника. Если раньше информационная безопасность в основном связывалась с защитой информационных систем и каналов передачи данных, то сегодня все большее значение имеет поведение человека, который непосредственно работает с цифровой средой.

Особую актуальность эта проблема приобретает в связи с использованием искусственного интеллекта. ИИ активно применяется как инструмент обработки больших массивов информации, поиска взаимосвязей, анализа цифровых следов и

повышения эффективности правоохранительной деятельности. Исследования казахстанских авторов также показывают, что искусственный интеллект уже рассматривается применительно к следственной практике как инструмент анализа данных, выявления закономерностей и ускорения работы правоохранительных органов. При этом ИИ рассматривается не как замена сотрудника, а как вспомогательный инструмент его деятельности [2].

В Республике Казахстан этот процесс уже приобретает практический характер. В 2026 году МВД Республики Казахстан развивает ИИ-компетенции сотрудников и проводит практическое обучение по созданию ИИ-агентов, автоматизации рабочих процессов и разработке цифровых решений с учетом специфики деятельности органов внутренних дел.

Государственными документами также предусмотрено развитие аналитической платформы МВД с использованием алгоритмов машинного обучения и интеграция в ЕРДР модуля «Цифровой помощник следователя» на основе ИИ [3].

Таким образом, сотрудник полиции становится непосредственным участником новой системы взаимодействия «человек – данные – искусственный интеллект». В этих условиях его цифровое поведение приобретает особое значение. От того, как сотрудник работает с информацией, что размещает в сети и какие цифровые инструменты использует, может зависеть не только сохранность информации, но и его личная и профессиональная безопасность.

Цель настоящего исследования заключается в обосновании необходимости рассматривать цифровое поведение сотрудника полиции как самостоятельный фактор его профессиональной безопасности при использовании технологий искусственного интеллекта.

Основная часть. Информационная безопасность традиционно основывается на обеспечении конфиденциальности, целостности и доступности информации. Однако применительно к деятельности полиции такого подхода, по нашему мнению, уже недостаточно.

Угроза может возникнуть не только из-за технической уязвимости информационной системы. Источником риска может стать сам сотрудник. Например, если он публикует сведения о месте службы, раскрывает геолокацию, размещает фотографии в форме, сообщает информацию о коллегах или использует незащищенный цифровой ресурс для передачи служебных сведений.

Поэтому цифровое поведение следует понимать шире, чем просто соблюдение правил работы с информационными технологиями. И. С. Лучинкина под цифровым поведением понимает «активность субъекта или его цифрового образа в цифровой среде, которая проявляется во взаимодействии субъектов или их цифровых образов. Цифровое поведение личности или её цифрового образа характеризуется качественным составом участников взаимодействия, радиусом взаимодействия и интенсивностью взаимодействия» [4, с. 56].

Применительно к сотрудникам полиции цифровое поведение можно рассматривать как совокупность действий в цифровой среде, посредством которых сотрудник создает, получает, передает, хранит и распространяет информацию.

Особенность такого поведения связана с профессиональным статусом сотрудника. Личная цифровая активность не всегда остается только личной. Информация, размещенная сотрудником с собственного аккаунта вне рабочего времени, при определенных обстоятельствах может быть связана пользователями с его служебным статусом.

В этом случае возникает прямая связь между цифровым следом сотрудника и его профессиональной безопасностью. Например, отдельно взятая фотография с места отдыха может не представлять серьезной опасности. Но если в социальных сетях регулярно размещаются фотографии, по которым можно определить место проживания, автомобиль, членов семьи, место службы и обычные маршруты сотрудника, совокупность этих сведений уже позволяет сформировать достаточно подробный цифровой профиль.

Раньше такой анализ требовал значительных временных ресурсов. Сегодня искусственный интеллект способен значительно ускорить сопоставление информации и выявить взаимосвязи между отдельными сведениями.

Поэтому проблема заключается не только в том, какую именно информацию сотрудник размещает в сети. Важно и то, какие дополнительные выводы можно сделать из совокупности открытых данных с помощью современных технологий анализа.

Еще одним риском становится распространение недостоверного цифрового контента. Возможность создавать реалистичные изображения и аудиовизуальные материалы может использоваться для дискредитации сотрудника полиции или создания ложного представления о его действиях. В результате цифровая среда может стать не только источником утечки информации, но и инструментом формирования угроз для репутации и профессиональной деятельности сотрудника.

Отдельного внимания требует ситуация, когда источником риска становится не преступник, а неправильное использование самим сотрудником искусственного интеллекта.

Практическая привлекательность генеративных ИИ-сервисов очевидна. Сотрудник может использовать их для подготовки проекта документа, сокращения текста, перевода, систематизации информации или поиска идей. Однако при работе с такими сервисами возникает важный вопрос: какие именно данные можно передавать системе?

Если сотрудник загружает в открытый ИИ-сервис документ, содержащий персональные данные, сведения о сотрудниках, материалы проверки, данные досудебного расследования или другую информацию ограниченного доступа, он фактически создает дополнительный канал обработки этой информации.

Поэтому цифровая гигиена в деятельности полиции должна строиться на простом принципе: «не передавай в ИИ то, что не вправе передавать третьему лицу». Этот подход также должен основываться на требованиях законов Республики Казахстан «О персональных данных и их защите» и «Об искусственном интеллекте».

Именно эти обстоятельства позволяют рассматривать цифровое поведение сотрудника полиции как криминологически значимый фактор профессиональной безопасности.

Казахстанские исследователи Н.В. Сидорова, Н.О. Дулатбеков и Л.К. Кусаинова справедливо отмечают необходимость рассматривать искусственный интеллект не только как технологическое средство, но и как самостоятельную правовую категорию, требующую соответствующего регулирования при его использовании в судебной и правоохранительной деятельности [5].

Проблема безопасного использования ИИ характерна не только для Казахстана. Современные международные подходы рассматривают ответственное использование искусственного интеллекта в правоохранительной деятельности как отдельную организационную задачу. INTERPOL и UNICRI в обновленном в 2024 году *Toolkit for Responsible AI Innovation in Law Enforcement* акцентируют внимание не только на технических возможностях ИИ, но и на управлении рисками, этике, правах человека и готовности правоохранительных организаций к безопасному внедрению технологий [6].

В связи с этим специальное ведомственное регулирование применения генеративного ИИ сотрудниками органов внутренних дел представляется необходимым. При этом, на наш взгляд, недостаточно просто запретить сотрудникам использование отдельных сервисов. Более эффективной может быть дифференцированная модель, при которой сотрудник понимает, какую информацию можно обрабатывать с помощью ИИ, какую информацию допускается обрабатывать только в защищенной ведомственной системе, а какую вообще нельзя передавать в ИИ-сервисы.

Такой подход позволит перейти от формального запрета к формированию осознанного цифрового поведения.

В исходном исследовании цифровая гигиена рассматривается как способность сотрудника самостоятельно распознавать потенциальную угрозу и предотвращать ее до наступления негативных последствий. Данный подход представляется обоснованным, однако в современных условиях его содержание необходимо расширить.

Речь должна идти не только о паролях, многофакторной аутентификации, подозрительных ссылках и настройках приватности. Сотрудник должен уметь оценивать цифровую информацию с позиции возможного криминального использования.

Перед публикацией информации сотрудник должен понимать, может ли она раскрыть место его службы, местонахождение, круг общения, сведения о семье или характер выполняемых задач. При работе с ИИ появляется еще один критерий: является ли используемая информационная система разрешенным и защищенным инструментом для обработки соответствующих данных.

В этой связи перспективной представляется простая модель «остановись – оцени –проверь». Перед публикацией или передачей информации сотрудник должен оценить ее содержание, возможные последствия распространения и круг лиц, которые потенциально получат к ней доступ. Перед использованием ИИ необходимо дополнительно проверить, разрешено ли передавать конкретную информацию выбранному сервису.

Заключение. Проведенный анализ показывает, что цифровое поведение сотрудника полиции необходимо рассматривать как часть системы обеспечения его

профессиональной безопасности. В условиях активного внедрения ИИ значение этого вопроса будет только возрастать.

Для этого необходимо разработать ведомственные правила цифрового поведения сотрудников органов внутренних дел. В них следует отдельно определить требования к использованию социальных сетей, фотографий, геолокации, мессенджеров, персональных данных и искусственного интеллекта.

Одновременно в профессиональную подготовку сотрудников целесообразно включить практический модуль по цифровой гигиене и безопасному использованию ИИ. Важно оценивать не только знание правил, но и способность сотрудника правильно действовать в конкретной цифровой ситуации.

Не менее важна защищенная цифровая инфраструктура. Если сотруднику предоставляется безопасный ведомственный инструмент для решения профессиональных задач с использованием ИИ, необходимость обращения к внешним сервисам снижается.

При этом должен сохраняться принцип человеческого контроля. ИИ может использоваться для анализа и обработки информации, но его результат не должен автоматически восприниматься как окончательный и достоверный. Исследования применения ИИ в правоохранительной сфере также подчеркивают вспомогательный характер таких технологий по отношению к профессиональному решению сотрудника.

Таким образом, безопасное цифровое поведение должно стать частью профессиональной культуры сотрудника полиции. Сотрудник должен понимать, что любое цифровое действие оставляет информационный след. В условиях искусственного интеллекта этот след может быть быстро собран, сопоставлен и использован. Поэтому цифровая гигиена и безопасное взаимодействие с ИИ следует рассматривать как новое направление профилактики угроз профессиональной безопасности сотрудников органов внутренних дел.

Список литературы:

1. Полиция Казахстана раскрыла детали про свои передовые цифровые технологии [Электронный-ресурс]. URL: https://kaztag.kz/ru/news/politsiya-kazakhstana-raskryla-detali-pro-svoi-peredovye-tsifrovye-tekhnologii

2. Байгелова Н.Е., Жумадилла А.К., Үркімбай Қ.Б. Цифровизация правоохранительной деятельности: использование искусственного интеллекта в следственной практике // Вестник КазНПУ имени Абая. Серия: Международная жизнь и политика. 2025. № 80.

3. Вайбкодинг в МВД: Масштабное развитие AI-компетенций сотрудников [Электронный- ресурс]. URL: https://www.gov.kz/memleket/entities/maidd/press/news/details/1268267?lang=ru

4. Лучинкина, И. С. Поведение личности в современной цифровой среде / И. С. Лучинкина // Инновационная наука: Психология. Педагогика. Дефектология. — 2023. — № 6. — С. 51—58

5. Сидорова Н.В., Дулатбеков Н.О., Кусаинова Л.К. Искусственный интеллект как правовая категория и объект правового регулирования // Вестник Карагандинского университета. Серия «Право». 2024. Т. 29. № 3 (115). С. 78–90.

6. Interpol – Responsible AI in Law Enforcement [Электронный-ресурс]. URL:https://regulations.ai/regulations/RAI-X8-GO-RESPONS-2024

ЕСЕНБАЕВА АРАЙЛЫМ ЛЕМИСОВНА
Старший преподаватель
кафедры факультета развития профессиональных компетенций
Академии КНБ Республики Казахстан

КИБЕРБЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РЕСПУБЛИКИ КАЗАХСТАН: СОВРЕМЕННЫЕ УГРОЗЫ И МЕХАНИЗМЫ ЗАЩИТЫ

Цифровизация ключевых отраслей экономики и государственного управления Республики Казахстан сопровождается повышением зависимости общественно значимых процессов от информационных и телекоммуникационных технологий. Энергетика, транспорт, финансовый сектор, связь, здравоохранение и государственные информационные системы в значительной степени используют цифровые платформы и автоматизированные системы управления. В результате устойчивость функционирования критически важных объектов все в большей степени определяется их способностью противостоять современным киберугрозам.

Особую опасность представляют кибератаки, направленные на критическую инфраструктуру, поскольку их последствия могут выходить далеко за пределы отдельных информационных систем. Нарушение работы цифровой системы управления энергетическим объектом, транспортной инфраструктурой или телекоммуникационной сетью потенциально способно привести к остановке технологических процессов, финансовым потерям, нарушению предоставления общественно значимых услуг и возникновению более широких социальных последствий. Таким образом, кибербезопасность критической инфраструктуры приобретает значение не только технической, но и экономической и национальной безопасности.

Современный характер киберугроз также усложняется использованием вредоносного программного обеспечения, атак на цепочки поставок, социальной инженерии, эксплуатации уязвимостей технологических систем и компрометации учетных данных. При этом уязвимость может возникать не только вследствие недостаточной защищенности оборудования или программного обеспечения, но и в результате ошибок персонала, недостаточного уровня подготовки специалистов и отсутствия эффективных процедур реагирования на инциденты.

В этих условиях традиционного подхода, ориентированного преимущественно на предотвращение кибератак, становится недостаточно. Современная система защиты должна обеспечивать не только предотвращение угроз, но и их своевременное обнаружение, локализацию последствий, восстановление функционирования и последующий анализ инцидента. Поэтому все большее значение приобретает концепция киберустойчивости, предполагающая способность критической инфраструктуры сохранять или оперативно восстанавливать основные функции даже в условиях успешной кибератаки.

Для Республики Казахстан данная проблема имеет особое значение в связи с продолжающейся цифровизацией экономики, государственного управления и

социально значимых услуг. Повышение уровня защищенности критической инфраструктуры требует комплексного подхода, включающего технологические, организационные, кадровые и нормативно-правовые меры. При этом особое внимание должно уделяться взаимодействию государства, операторов критически важных объектов и специалистов в области информационной безопасности.

Степень разработанности проблемы характеризуется значительным количеством исследований в области защиты критической информационной инфраструктуры, управления киберрисками и киберустойчивости. Вместе с тем применительно к Казахстану сохраняется необходимость комплексного рассмотрения современных угроз критической инфраструктуре и определения практических направлений повышения ее устойчивости к киберинцидентам.

Цель исследования — определить основные угрозы кибербезопасности критической инфраструктуры Республики Казахстан и предложить направления совершенствования механизмов ее защиты и киберустойчивости.

Для достижения поставленной цели определены следующие задачи исследования:

1. рассмотреть особенности критической инфраструктуры в условиях цифровизации;
2. определить основные современные киберугрозы критически важным объектам;
3. проанализировать существующие механизмы обеспечения кибербезопасности в Казахстане;
4. выявить основные технологические, организационные и кадровые уязвимости;
5. определить перспективные направления повышения киберустойчивости критической инфраструктуры Республики Казахстан.

Методы исследования. В работе использованы системный, аналитический и сравнительный методы, а также анализ нормативных документов и научной литературы в области кибербезопасности и защиты критической инфраструктуры. Системный подход позволил рассмотреть критическую инфраструктуру как совокупность взаимосвязанных технологических и организационных элементов, а аналитический метод — определить основные угрозы и направления совершенствования механизмов киберустойчивости.

Критическая инфраструктура представляет собой совокупность объектов и систем, устойчивое функционирование которых имеет существенное значение для жизнедеятельности общества, экономики и государства. В условиях цифровизации значительная часть процессов управления такими объектами осуществляется посредством информационных систем, телекоммуникационных сетей и автоматизированных технологических решений. Поэтому нарушение цифровой составляющей может непосредственно повлиять на физическое функционирование инфраструктуры.

К числу наиболее чувствительных с точки зрения кибербезопасности относятся энергетика, транспорт, связь, финансовый сектор, здравоохранение и государственные информационные системы. Их взаимосвязанность формирует дополнительный риск: нарушение работы одного элемента способно вызвать

цепную реакцию и затронуть другие системы. Например, сбой телекоммуникационной инфраструктуры может осложнить функционирование финансовых сервисов и государственных информационных ресурсов.

Особую проблему создает использование устаревших информационных и технологических систем, которые не всегда изначально проектировались с учетом современных требований к кибербезопасности. Их модернизация может быть сложной и дорогостоящей, а полная замена — невозможной без временного нарушения технологических процессов. В результате формируется ситуация, при которой цифровая инфраструктура развивается быстрее, чем механизмы ее защиты.

Кроме того, критические объекты становятся частью единого цифрового пространства, взаимодействуя с внешними поставщиками, подрядчиками, облачными сервисами и телекоммуникационными операторами. Это расширяет функциональные возможности систем, но одновременно увеличивает количество потенциальных точек входа для злоумышленников.

Современная критическая инфраструктура сталкивается с широким спектром киберугроз, способных нарушить работу информационных и технологических систем. Одной из наиболее распространенных угроз остается использование вредоносного программного обеспечения, включая программы-вымогатели, которые могут привести к блокированию информационных ресурсов, нарушению доступа к данным и остановке отдельных процессов.

Особую опасность представляют атаки на промышленные системы управления и технологическую инфраструктуру. В отличие от обычных информационных систем, нарушение работы таких объектов может иметь непосредственные физические последствия. Компрометация систем управления способна привести к нарушению технологических процессов, поэтому их защита требует особого уровня контроля и сегментации.

Отдельную категорию составляют атаки на цепочки поставок. Современные организации используют большое количество программных продуктов, оборудования и внешних сервисов. Компрометация одного поставщика потенциально может предоставить злоумышленнику доступ сразу к нескольким связанным организациям. Таким образом, безопасность критической инфраструктуры зависит не только от собственных защитных механизмов объекта, но и от уровня защищенности его внешних контрагентов.

Существенным фактором риска остается социальная инженерия. Фишинговые сообщения, кража учетных данных и манипулирование сотрудниками позволяют обходить технические механизмы защиты посредством воздействия непосредственно на человека. В результате даже технологически защищенная система может оказаться уязвимой при недостаточном уровне подготовки персонала.

Отдельную проблему представляют уязвимости устаревшего программного обеспечения и оборудования, отсутствие своевременных обновлений, неправильная настройка систем и недостаточная сегментация сетевой инфраструктуры. Совокупность этих факторов увеличивает поверхность атаки и усложняет своевременное обнаружение угроз.

Обеспечение кибербезопасности критической инфраструктуры Республики Казахстан предполагает сочетание нормативно-правовых, организационных и технических механизмов. При этом защита должна быть ориентирована не только на предотвращение несанкционированного доступа, но и на постоянный мониторинг состояния информационных систем, своевременное выявление угроз и обеспечение готовности к реагированию на инциденты.

Важное значение имеет установление требований к субъектам, эксплуатирующим критически важные информационные и технологические объекты. Такие требования должны охватывать управление киберрисками, защиту информационных ресурсов, контроль доступа, резервное копирование данных, обновление программного обеспечения и регулярную оценку защищенности систем.

Отдельным элементом является мониторинг киберугроз. Постоянное наблюдение за сетевой активностью и состоянием информационных систем позволяет выявлять аномальное поведение на ранних стадиях. При этом эффективность мониторинга определяется не только техническими средствами обнаружения, но и способностью специалистов оперативно интерпретировать полученную информацию и принимать соответствующие меры.

Не менее важным является наличие механизмов реагирования на компьютерные инциденты. Критическая инфраструктура должна иметь заранее определенные процедуры действий при обнаружении атаки: идентификацию источника угрозы, локализацию скомпрометированного сегмента, сохранение необходимых данных, восстановление функционирования и последующий анализ произошедшего.

Особую роль играет межведомственное взаимодействие. Кибератака на критический объект потенциально может затрагивать интересы нескольких организаций и государственных органов. Поэтому обмен информацией об обнаруженных угрозах, уязвимостях и способах атак позволяет повысить эффективность коллективной защиты и сократить время реагирования.

Таким образом, система защиты критической инфраструктуры должна функционировать как непрерывный цикл:

мониторинг → обнаружение → анализ → реагирование → восстановление → анализ инцидента → совершенствование защиты.

Такой подход позволяет перейти от преимущественно реактивной модели к системе постоянного управления киберрисками и формирует основу для повышения общей киберустойчивости критической инфраструктуры Казахстана.

Несмотря на развитие механизмов обеспечения кибербезопасности, критическая инфраструктура сохраняет ряд уязвимостей, связанных с технологическими, организационными и человеческими факторами. Одной из основных проблем является использование устаревших информационных и технологических систем, модернизация которых может быть затруднена их высокой стоимостью, сложностью замены и необходимостью непрерывного функционирования объектов.

Существенным риском остается недостаточная сегментация информационных сетей. При отсутствии эффективного разделения корпоративных,

административных и технологических систем компрометация одного сегмента может создать условия для дальнейшего распространения атаки. Поэтому изоляция критически важных технологических компонентов и строгий контроль внешних подключений являются важными элементами защиты.

Отдельной проблемой выступает кадровый фактор. Эффективная киберзащита требует специалистов, обладающих одновременно техническими знаниями, пониманием специфики конкретной отрасли и навыками реагирования на инциденты. Недостаток таких специалистов способен снижать эффективность даже современных технических средств защиты.

Не менее значимым остается человеческий фактор. Ошибки сотрудников, недостаточная осведомленность о методах социальной инженерии, использование ненадежных учетных данных и несоблюдение внутренних процедур могут создавать возможности для проникновения в защищенные системы.

Наконец, одной из системных проблем является ориентация исключительно на предотвращение атаки. Даже развитая система защиты не способна гарантировать абсолютное отсутствие киберинцидентов. Поэтому критически важным становится наличие механизмов быстрого обнаружения, локализации и восстановления после успешной атаки.

Повышение киберустойчивости критической инфраструктуры требует перехода от преимущественно превентивной модели защиты к комплексному подходу, учитывающему весь цикл возникновения и развития киберинцидента. Основной задачей становится не только предотвращение атаки, но и способность инфраструктуры своевременно обнаружить угрозу, ограничить ее распространение, восстановить основные функции и использовать полученный опыт для совершенствования системы защиты.

Одним из приоритетных направлений является усиление сегментации критических информационных и технологических систем. Разделение сетей и ограничение взаимодействия между отдельными компонентами позволяют снизить вероятность распространения атаки в случае компрометации одного из элементов. Особое внимание необходимо уделять контролю удаленного доступа и подключений внешних организаций.

Важное значение имеет регулярное стресс-тестирование киберустойчивости. Имитация различных сценариев кибератак позволяет проверить не только эффективность средств обнаружения, но и готовность персонала к реагированию, работу резервных систем и способность объекта восстановить критически важные процессы. Такие мероприятия целесообразно проводить регулярно, поскольку характер киберугроз постоянно изменяется.

Отдельным направлением должно стать развитие кадрового потенциала. Необходимы специалисты, способные одновременно работать с информационной безопасностью, промышленными системами управления, цифровой криминалистикой и реагированием на инциденты. Параллельно следует повышать общий уровень культуры кибербезопасности сотрудников критически важных объектов, поскольку технические средства защиты не исключают риска социальной инженерии и человеческих ошибок.

Представляется целесообразным развивать и систему обмена информацией о киберугрозах между государственными органами и операторами критической инфраструктуры. Своевременное получение сведений о новых уязвимостях, способах атак и индикаторах компрометации позволит сокращать время между обнаружением угрозы и принятием защитных мер.

В результате перспективную модель киберустойчивости критической инфраструктуры можно представить следующим образом:

идентификация рисков → предотвращение → обнаружение → реагирование → локализация → восстановление → анализ инцидента → совершенствование защиты.

Проведенный анализ показывает, что цифровизация критической инфраструктуры Республики Казахстан одновременно повышает эффективность управления и создает новые зависимости от информационных и телекоммуникационных технологий. В результате кибератаки на отдельные элементы инфраструктуры могут иметь последствия, выходящие за пределы одной информационной системы и затрагивающие устойчивость общественно значимых процессов.

Основными угрозами выступают вредоносное программное обеспечение, атаки на технологические системы, компрометация цепочек поставок, социальная инженерия, эксплуатация уязвимостей устаревших систем и ошибки персонала. Их комплексный характер требует сочетания технологических, организационных и кадровых мер защиты.

Проведенное исследование позволяет сделать вывод, что обеспечение безопасности критической инфраструктуры не должно ограничиваться предотвращением кибератак. Необходима способность своевременно обнаруживать угрозу, локализовать ее последствия, восстанавливать функционирование и совершенствовать защиту на основе анализа произошедших инцидентов.

Для Казахстана перспективным является переход к модели киберустойчивости, основанной на постоянном управлении рисками, сегментации критических систем, регулярном стресс-тестировании, развитии кадрового потенциала и обмене информацией о киберугрозах между государственными органами и операторами инфраструктуры.

Список литературы:

1. Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК. – URL: https://adilet.zan.kz/rus/docs/K2600000255 (дата обращения: 18.08.2026).

2. Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры: приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 июня 2023 года № 221/НҚ. – URL: https://adilet.zan.kz/rus/docs/V2300032996 (дата обращения: 18.08.2026).

3. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 (с изменениями и дополнениями). – URL: https://www.adilet.zan.kz/rus/docs/P1600000832 (дата обращения: 18.08.2026).

4. Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры: приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 14 марта 2018 года № 48/НҚ. – URL: https://adilet.zan.kz/rus/docs/V1800017019 (дата обращения: 18.08.2026).

5. Концепция цифровой трансформации, развития отрасли информационных технологий и кибербезопасности на 2023–2029 годы: утверждена постановлением Правительства Республики Казахстан от 28 марта 2023 года № 269. – URL: https://www.gov.kz/memleket/entities/infsecurity/press/article/details/95401 (дата обращения: 18.08.2026).

6. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. – Gaithersburg: National Institute of Standards and Technology, 2021. – 304 p. – (NIST Special Publication 800-160, Vol. 2, Rev. 1). – DOI: 10.6028/NIST.SP.800-160v2r1.

7. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. – Gaithersburg: NIST, 2024. – 49 p. – DOI: 10.6028/NIST.CSWP.29.

8. International Organization for Standardization. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva: ISO, 2022.

9. International Organization for Standardization. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. – Geneva: ISO, 2022.

10. World Economic Forum. Global Cybersecurity Outlook 2025. – Geneva: World Economic Forum, 2025. – 34 p. – URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (дата обращения: 18.08.2026).

ЖАНХАН НҰРБАҚЫТ ЖАНХАНҰЛЫ
Қазақстан Республикасы ІІМ Басқару академиясының
Ғылыми-зерттеу институты
ІІО жедел-іздестіру қызметін және киберқылмысқа
қарсы іс-қимылды зерттеу орталығының бастығы
заң ғылымдарының магистрі, полиция полковнигі

ЖЕДЕЛ-ІЗДЕСТІРУ ҚЫЗМЕТІН АҚПАРАТТЫҚ-ТАЛДАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТІНІ ҚОЛДАНУДЫҢ ҚҰҚЫҚТЫҚ ЖӘНЕ ҰЙЫМДАСТЫРУШЫЛЫҚ НЕГІЗДЕРІ

Кіріспе

Қылмыстық ортаның цифрлануы, коммуникация арналарының көбеюі және оқиғалар туралы мәліметтің жоғары жылдамдықпен жаңаруы жедел-іздестіру органдарының ақпараттық жұмысын күрделендіреді. Талдаушы бір мезгілде мәтіндік хабарламаларды, оқиғалар хронологиясын, нысандар арасындағы байланыстарды және географиялық деректерді салыстыруға мәжбүр. Мұндай жағдайда жасанды интеллект адамның кәсіби пайымын алмастыратын құрал емес, ақпараттық шуды азайтып, тексеруге жататын белгілерді жылдам бөліп көрсететін технология ретінде құнды. Қазақстан Республикасында жасанды интеллектіні дамыту тұжырымдамалық және заңнамалық деңгейде бекітілуі осы мәселені жедел қызметтің арнайы құқықтық табиғатын ескере отырып зерттеуді өзекті етеді [2; 4].

Зерттеудің ғылыми проблемасы жасанды интеллектінің техникалық мүмкіндігі мен жедел-іздестіру қызметіндегі құқықтық жауапкершіліктің бөлінбейтін сипаты арасындағы қайшылықтан туындайды. Алгоритм ықтимал сәйкестікті немесе тәуекелді есептей алады, бірақ дерек жинаудың заңдылығын, шараның қажеттілігі мен мөлшерлестігін, сондай-ақ нақты адамға қатысты шешімнің құқықтық салдарын өздігінен бағалай алмайды. Сондықтан дәлдігі жоғары модельдің өзі құқықтық рәсім әлсіз болған жағдайда жаңсақ күдікті күшейтуі, бастапқы деректегі бұрмалауды қайталауы немесе тексерілмеген қорытындыны беделді факт ретінде көрсетуі мүмкін.

Зерттеудің мақсаты – жедел-іздестіру қызметін ақпараттық-талдамалық қамтамасыз етуде жасанды интеллектіні қолданудың жол берілетін шегін айқындау және құқықтар мен қауіпсіздікке әсер ететін шешімдер үшін тексерілетін басқару моделін ұсыну. Осы мақсатқа жету үшін ЖИ құралдарының негізгі функциялары жүйеленді; ұлттық құқық нормалары мен халықаралық ұсынымдар салыстырылды; деректер, модель және шешім деңгейіндегі тәуекелдер бөлінді; практикалық енгізудің рәсімдік кепілдіктері тұжырымдалды. Зерттеу ашық нормативтік және ғылыми материалдарға негізделді, ал арнайы қызметтің жабық әдістері мен нақты операциялық деректері талдау пәніне енгізілген жоқ.

Жасанды интеллектінің ақпараттық талдаудағы функционалдық мүмкіндіктері

Жедел-іздестіру қызметіндегі ақпараттық талдаудың бастапқы міндеті – әртүрлі дереккөздерден түскен мәліметті ортақ контекстке келтіру. ЖИ

технологиялары бұл жұмыста төрт өзара байланысты бағыт бойынша қолданылуы мүмкін. Біріншісі – табиғи тілді өңдеу арқылы құжаттарды тақырып бойынша жіктеу, атауларды, уақытты, мекенді және өзге нысандарды бөліп алу, көптілді мәтіндердегі ұқсастықтарды табу. Қазақ және орыс тілдеріндегі материалдар үшін терминологиялық сөздіктер, морфологиялық ерекшеліктер және контекстік мағына бөлек тексерілуге тиіс.

Екінші бағыт – графтық талдау. Ол адамдар, байланыс құралдары, оқиғалар, ұйымдар және цифрлық нысандар арасындағы қатынастарды желі түрінде бейнелеп, жасырын емес, бірақ қолмен байқауы қиын құрылымдық байланыстарды анықтауға мүмкіндік береді. Мұнда байланыс фактісі қылмысқа қатыстылықты білдірмейді. Графтық өлшемдер тек қосымша тексеруді қажет ететін нүктелерді көрсетеді; олардың мәні деректің толықтығына, өзектілігіне және заңды алынуына тәуелді.

Үшінші бағыт – уақыттық және кеңістіктік заңдылықтарды талдау. Оқиғалардың қайталану мерзімі, маршруттардың қиылысуы немесе әрекеттердің реттілігі талдаушыға бірнеше нұсқаны салыстыруға көмектеседі. Алайда ықтималдық үлгісі өткен деректердің құрылымын жалғастырады; ол болашақ оқиғаны дәлелденген факт ретінде болжамайды. Осы ерекшелік ескерілмесе, бұрын жиі тексерілген аумақтар мен топтар туралы деректер жаңа тексерулерді қайтадан сол нысандарға бағыттайтын тұйық кері байланыс қалыптастыруы мүмкін [8; 9].

Төртінші бағыт – талдамалық құжат дайындауды қолдау. Генеративті модельдер көлемді мәтінді қысқаша мазмұндауға, оқиғалар хронологиясын бастапқы жоба ретінде құрастыруға, қарама-қайшы мәліметтерді көрсетуге және іздеу сұрауларын ұсынуға қабілетті. Бірақ мұндай модель ықтимал тілдік жалғастыруды жасайды және жоқ деректі сенімді түрде құрастыруы мүмкін. Сондықтан әрбір тұжырым бастапқы материалға кері сілтememен расталып, дәйексөз, күн, тұлға және құқықтық реквизит адаммен қайта тексерілуге тиіс. NIST генеративті ЖИ профилі де жалған мазмұн, ақпараттық қауіпсіздік және адамның технологияға шамадан тыс сенуі сияқты арнайы тәуекелдерді бөлек басқаруды ұсынады [7].

Көрсетілген мүмкіндіктердің ортақ сипаты – олардың бағдарлаушы болуы. ЖИ талдаушыға нұсқа, байланыс немесе сәйкессіздік ұсынады, бірақ жедел болжамды тексерудің, деректің контекстін түсіндірудің және заңда көзделген негізді анықтаудың орнына жүрмейді. Тиімділік бір ғана дәлдік көрсеткішімен емес, қате оң және қате теріс нәтижелердің салдарымен, нәтижені қайта өндіру мүмкіндігімен, жауапты тұлғаның оны түсіндіре алуымен және шешімге дейінгі уақыттың негізді қысқаруымен өлшенуге тиіс.

Құқықтық шектер және алгоритм нәтижесінің мәртебесі

Қазақстан Республикасының «Жедел-іздестіру қызметі туралы» Заңы заңдылықты, адамның құқықтары мен бостандықтарын сақтауды жедел-іздестіру қызметінің қағидаттары ретінде бекітеді. Заңда жедел-іздестіру іс-шараларын жүргізу негіздері, алынған материалдарды пайдалану тәртібі және жедел есепке алу істерін жүргізу көзделген [1]. Демек, ақпараттық жүйеде белгілі бір белгі анықталуы заңда жоқ жаңа негізді туындатпайды. Алгоритмдік нәтиже қолданыстағы құқықтық негізді және уәкілетті адамның жауапкершілігін алмастыра алмайды.

Аталған Заңның жедел-іздестіру қызметінің нәтижелерін пайдалану жөніндегі талаптары материалдың қылмыстық процесте заңда белгіленген тәртіппен тексерілуін көздейді; тиісті процестік нысанға келтірілмеген материалдың құқықтарды шектеуге тікелей негіз болуына жол берілмейді [1]. Бұл қағида ЖИ көмегімен алынған қорытындыға да қолданылуға тиіс: машина ұсынған сәйкестік, тәуекел балы немесе байланыс кестесі бастапқы дерекпен расталып, оның қалай алынғаны мен қандай қателік ықтималдығы бар екені бағаланбайынша дербес құқықтық мағынаға ие болмайды.

«Жасанды интеллект туралы» Заң әділдік пен теңдік, ашықтық пен түсініктілік, жауапкершілік пен бақылау және адамның дербестігі қағидаттарын бекітеді. Сондай-ақ жүйелерді тәуекел деңгейі бойынша жіктеу, қолжетімділігі шектеулі ақпарат пайдаланылған кезде оқшауланған инфрақұрылымда жұмыс істеу және аудит жүргізу мәселелері реттелген [2]. Бұл нормалар жедел-іздестіру саласында ЖИ жүйесін сатып алу кезеңінен бастап талаптарды белгілеуді қажет етеді: модельдің мақсаты, дерек санаттары, рұқсат етілген пайдаланушылар, журналдау, жаңарту тәртібі және тоқтату шарттары алдын ала анықталуы керек.

«Дербес деректер және оларды қорғау туралы» Заңның 19-1-бабы адамның құқықтары мен заңды мүдделерін қозғайтын, тек автоматтандырылған өңдеуге негізделген шешімдерге жалпы шектеу қояды; ерекшелік субъектінің келісімімен не заңда көзделген жағдайда ғана мүмкін [3]. Жедел-іздестіру ақпараты үшін бұл талап деректерді өңдеудің құқықтық негізін, мақсатқа сәйкестігін және қолжетімділікті қатаң ажыратуды білдіреді. Техникалық мүмкіндік мәліметті жинауға немесе біріктіруге өздігінен заңды өкілеттік бермейді.

Осы зерттеуде алгоритмдік-талдамалық сигнал деп ЖИ жүйесінің бастапқы мәліметтер арасындағы ықтимал сәйкестік, байланыс, ауытқу немесе тәуекел туралы қалыптастырған, міндетті адами тексеруді қажет ететін бағдарлаушы нәтижесі түсініледі. Бұл ұғым қолданыстағы заңдағы дәлелдемені, жедел ақпаратты немесе шешімді алмастырмайды. Оның ғылыми мәні – машиналық қорытынды мен одан кейінгі құқықтық әрекеттің арасына тексеру рәсімін енгізу. Сигналдың міндетті белгілері ретінде дереккөзге сілтеме, модель нұсқасы, есептелген уақыт, сенімділік көрсеткіші, белгілі шектеулер және тексеруші қызметкердің қорытындысы тіркелуге тиіс.

Негізгі тәуекелдер

Бірінші тәуекел – деректің заңсыз немесе мақсатқа сай емес пайдаланылуы. Бірнеше дерекқорды біріктіру әрқайсысында бөлек көрінбейтін жаңа, сезімтал профиль қалыптастыруы мүмкін. Сондықтан жүйеге енгізілетін әрбір дерек жиыны үшін құқықтық негіз, жинау мақсаты, сақтау мерзімі, сапа деңгейі және қолжетімді тұлғалар көрсетілген дерек паспорты болуы қажет. Шығу тегі белгісіз, ескірген немесе қайта тексеруге келмейтін мәлімет автоматтандырылған талдауға жіберілмеуге тиіс.

Екінші тәуекел – тарихи бұрмалаудың қайталануы. Болжамдық жүйе объективті болмысқа емес, өзіне берілген жазбаларға үйренеді. Егер деректер бұрынғы бақылау қарқындылығын, есепке алу тәртібін немесе толық тіркелмеген оқиғаларды көрсетсе, модель сол айырманы тәуекелдің нақты айырмасы деп қабылдауы мүмкін. Ғылыми әдебиетте полиция деректерінің өндірілген контекстін

елемеу болжам нәтижесін бұрмалайтыны және тарихи заңсыздықтарды техникалық үлгі арқылы қайта жаңғырту қаупі көрсетілген [8-10].

Үшінші тәуекел – түсіндірілмейтін нәтиже. Модельдің жалпы дәлдігі жоғары болғанымен, нақты адамға қатысты нәтиженің қандай белгілермен қалыптасқанын анықтау мүмкін болмаса, оны тексеру және даулауға жауап беру қиындайды. Дарем полициясының HART моделін талдаған зерттеу алгоритмдік тәуекелді бағалауда эксперименттік тексеру, пропорционалдық және шешім рәсімін қатар қарау керектігін көрсетеді [11]. Сондықтан жедел талдау жүйесінде түсіндіру техникалық сипаттама ғана емес, құқықтық бақылаудың шарты болуы тиіс.

Төртінші тәуекел – автоматтандыруға шамадан тыс сену. Уақыт тапшылығы кезінде қызметкер алгоритм ұсынған нұсқаны бейтарап немесе дәл деп қабылдауға бейім болуы мүмкін. Мұны төмендету үшін интерфейс сенімділік шегін, балама түсіндірулерді және жетіспейтін деректерді көрсетуге тиіс; қызметкер нәтижемен келіспеуге және оның себебін тіркеуге құқылы болуы керек. Құқықтарға елеулі әсер етуі ықтимал әрекет екінші тәуелсіз тексерушінің мақұлдауынсыз қабылданбауға тиіс.

Бесінші тәуекел – ақпараттық қауіпсіздік. Жедел мәліметті сыртқы жалпы мақсаттағы генеративті сервиске енгізу деректің бақылаудан шығуына әкелуі мүмкін. Сонымен бірге модельді оқыту дерегін уландыру, сұрау арқылы қорғаныстыайналып өту, құпия нұсқаулықты ашу және жеткізу тізбегіне араласу сияқты қатерлер бар. Қолжетімділігі шектеулі ақпаратпен жұмыс істейтін жүйе оқшауланған ортада орналастырылып, рөлдік қолжетімділік, шифрлау, журналдау, резервтік қалпына келтіру және оқиғаға ден қою рәсімдерімен қорғалуы қажет [2; 7].

Алтыншы тәуекел – жауапкершіліктің шашырауы. Жүйені әзірлеуші, дерек иесі, техникалық әкімші, талдаушы және шешім қабылдаушының міндеттері ажыратылмаса, қате нәтижеге кім жауап беретіні белгісіз қалады. NIST AI RMF басқару, өлшеу, картаға түсіру және тәуекелді басқару функцияларын ұйымның бүкіл өмірлік цикліне енгізуді ұсынады [6]. INTERPOL мен UNICRI құқық қорғау органдары үшін жауапты ЖИ инновациясын заңдылық, қажеттілік, мөлшерлестік және есептілік қағидаттарымен байланыстырады [5].

Авторлық құқыққа бағдарланған қолдану моделі

Ұсынылатын модель бес дәйекті кезеңнен және барлық кезеңге ортақ бақылау тетіктерінен тұрады. Бірінші кезеңде жедел міндет пен ЖИ қолданудың нақты мақсаты белгіленеді. Қандай сұраққа жауап ізделетіні, қандай нәтиже рұқсат етілетіні, қандай әрекетке ЖИ қорытындысын қолдануға болмайтыны жазбаша айқындалады. Мақсат кейіннен кеңейтілсе, құқықтық және тәуекелдік бағалау қайта жүргізіледі. Бұл талап функцияның байқалмай кеңеюіне және бір мақсат үшін жиналған деректің басқа мақсатқа негізсіз пайдаланылуына жол бермейді.

Екінші кезең – деректерді қабылдау қақпасы. Уәкілетті тұлға дерек жиынының заңды алынуын, мақсатқа қатыстылығын, уақыттық өзектілігін, толықтығын және бұрмалану қаупін тексереді. Әрбір жазбаның шығу тегін модель нәтижесіне дейін қадағалау мүмкін болуы қажет. Қате немесе даулы дерек анықталса, оны түзету, оқшаулау не есептеуден шығару туралы шешім журналға енгізіледі. Осы кезеңнен өтпеген мәліметтің көлемі көп болғанымен, ол талдаудың сенімді базасы болып саналмайды.

Үшінші кезең – бақыланатын алгоритмдік өңдеу. Модель тек бекітілген міндет пен рұқсат етілген деректер аясында жұмыс істейді. Жүйе нұсқасы, параметрлері, сұрау мәтіні, кіріс деректерінің идентификаторы және нәтиже уақыты автоматты түрде тіркеледі. Қолжетімділігі шектеулі ақпарат оқшауланған инфрақұрылымнан шығарылмайды. Модель жаңартылғанда оның алдыңғы нұсқамен салыстырғандағы қателік құрылымы, тұрақтылығы және қауіпсіздігі қайта сыналады.

Төртінші кезең – адами верификация және құқықтық саралау. Талдаушы алгоритмдік-талдамалық сигналды бастапқы дерекпен салыстырады, балама түсіндірулерді қарайды және расталмаған болжамды фактіден ажыратады. Егер кейінгі әрекет адамның құқықтары мен заңды мүдделеріне әсер етуі мүмкін болса, тәуелсіз екінші қызметкер құқықтық негізді, қажеттілікті және мөлшерлестікті тексереді. Соңғы шешімді лауазымды тұлға қабылдайды және алгоритм ұсынған нәтиже оның уәжін алмастырмайды.

Бесінші кезең – құжаттау, аудит және кейінгі мониторинг. Шешім журналында пайдаланылған дерек, модель нұсқасы, алгоритмдік нәтиже, тексеру қадамдары, келіспеу жағдайлары және қабылданған әрекет көрсетіледі. Кейін нақты нәтиже белгілі болғанда жалған оң және жалған теріс белгілер есептеліп, олар тіл, дерек түрі және қолдану сценарийі бойынша салыстырылады. Қателік шегі, қауіпсіздік оқиғасы немесе құқықтық талаптың бұзылуы анықталса, жүйені дереу тоқтатуға мүмкіндік беретін рәсім болуы керек.

Модельдің барлық кезеңіне үш көлденең кепілдік қолданылады. Біріншісі – модель паспорты: мақсат, әзірлеуші, дерек құрамы, тексеру нәтижелері, шектеулер және жауапты бөлімше көрсетіледі. Екіншісі – өзгермейтін аудит ізі: жүйеге кім, қашан және қандай мақсатпен кіргені, қандай нәтиже алғаны тіркеледі. Үшіншісі – құзыреттілік: оператор тек интерфейсті қолдануды емес, ықтималдықтың мәнін, қателік түрлерін, дербес деректер режимін және нәтижені даулаудың ішкі тәртібін білуге тиіс.

Ұсыныстың ғылыми жаңалығы үш тұжырымнан көрінеді. Біріншіден, алгоритмдік-талдамалық сигнал машиналық қорытындының құқықтық шешімнен бөлек, аралық ақпараттық мәртебесін айқындайды. Екіншіден, ЖИ нәтижесін жол берілетін пайдалану шарттары деректің дәлелді шығу тегі, нәтижені қайта тексеру, адами шешім, қауіпсіз орта, пропорционалдық және аудиттің жиынтығы ретінде негізделеді. Үшіншіден, тиімділікті бағалау техникалық дәлдікпен шектелмей, заңдық маңызы бар қателік құны, түсіндірілгіштік, тілдік теңдік және шешім ізінің толықтығы арқылы жүргізіледі.

Практикалық ұсыныстар

Біріншіден, жедел-іздестіру қызметінде ЖИ қолданудың ведомстволық тәртібін қабылдау ұсынылады. Құжаттың ашық бөлігінде негізгі қағидаттар, жауапкершілік, тәуекел санаттары және азаматтардың құқықтарына кепілдіктер белгіленіп, қолжетімділігі шектеулі қосымшада техникалық архитектура, дерек ағындары мен қауіпсіздік рәсімдері көрсетілуі мүмкін. Бұл тәсіл қызметтік құпияны сақтай отырып, қолданудың жалпы құқықтық шекарасын түсінікті етеді.

Екіншіден, жоғары тәуекелді әрбір қолдану сценарийіне алгоритмдік әсерді алдын ала бағалау енгізу қажет. Бағалау құқықтық негізді, мақсат пен баламаны,

дерек сапасын, ықтимал зардапты, кемсітушілік қаупін, киберқауіпсіздікті, адами бақылауды және шағымды қарау тетігін қамтуы тиіс. Еуропалық Одақтың ЖИ туралы актісіндегі жоғары тәуекелді жүйелерге қойылатын деректерді басқару, журналдау, техникалық құжаттама және адами қадағалау талаптары ұлттық модель үшін салыстырмалы бағдар бола алады [12].

Үшіншіден, тыйым салынатын сценарийлердің нақты тізбесін бекіту керек. Оған ЖИ нәтижесіне ғана сүйеніп адамды жедел есепке қою, жедел-іздестіру іс-шарасын бастау, құқықты шектеу, тұлғаның кінәлілігі туралы қорытынды жасау және шығу тегі белгісіз деректерден жасырын профиль қалыптастыру жатқызылуға тиіс. Мұндай шектеу технологиядан бас тартуды емес, оның функциясын заңда белгіленген адам өкілеттігінің шегінде ұстауды қамтамасыз етеді.

Төртіншіден, құқықтарға елеулі ықпал етуі ықтимал шешімдер үшін екі сатылы адами тексеру рәсімін енгізу қажет. Бірінші талдаушы дерек пен модель нәтижесінің сәйкестігін, екінші уәкілетті тұлға құқықтық негіз бен мөлшерлестікті тексереді. Екі қорытынды да қысқаша уәжбен тіркеледі. Бұл рәсім автоматтандыруға шамадан тыс сенуді төмендетіп, кейінгі ведомстволық және прокурорлық бақылауға тексерілетін материал береді.

Бесіншіден, деректер жиындары мен модельдердің бірыңғай ішкі тізілімін жүргізу ұсынылады. Онда жүйенің иесі, мақсаты, нұсқасы, тәуекел санаты, қолданылатын дерек, тест нәтижелері, инциденттер, жаңарту және тоқтату күні көрсетіледі. Тізілім бір функцияны бірнеше бөлімшенің бақылаусыз қайталап сатып алуын азайтып, жауапты тұлғаларды және нақты нұсқамен қабылданған шешімдерді анықтауға мүмкіндік береді.

Алтыншыдан, жүйелерді енгізу шектеулі пилоттан басталуы тиіс. Алғашқы кезеңде синтетикалық, иесіздендірілген немесе заңды ашық деректер қолданылып, қате оң және қате теріс нәтижелер, қазақ және орыс тілдеріндегі тұрақтылық, түсіндіру сапасы, өңдеу уақыты және қауіпсіздік оқиғалары өлшенеді. Пилот нәтижесін құқықтанушы, жедел қызмет маманы, деректер талдаушысы және ақпараттық қауіпсіздік маманы бірлесіп бағалағаннан кейін ғана нақты ортада қолдану туралы шешім қабылдануы керек.

Жетіншіден, жалпы қолжетімді генеративті сервистерге қызметтік және қолжетімділігі шектеулі ақпаратты енгізуге техникалық және ұйымдастырушылық тыйым қажет. Осындай деректермен жұмыс істейтін шешімдер оқшауланған ортада орналастырылып, рөлдік қолжетімділік пен сұраулар журналы міндетті болуы тиіс. Сегізіншіден, модель қатесі, дерек жылыстауы немесе негізсіз шешім анықталған жағдайда хабарлау, жүйені тоқтату, әсер еткен материалдарды қайта қарау және себепті жою тәртібі бекітілуі қажет.

Қорытынды

Жасанды интеллект жедел-іздестіру қызметін ақпараттық-талдамалық қамтамасыз етуде мәліметті жүйелеу, байланыстарды анықтау, мәтін мен оқиғалар хронологиясын өңдеу және талдамалық болжамдарды салыстыру мүмкіндігін кеңейтеді. Бірақ оның нәтижесі ықтималдық сипатта қалады және құқықтық негізді, адамның кәсіби бағасын немесе белгіленген рәсімді алмастырмайды. Сондықтан технологияның құндылығы автономдылық дәрежесімен емес, заңды әрі тексерілетін шешімге қаншалықты сапалы көмектесетінімен өлшенуге тиіс.

Ұсынылған алгоритмдік-талдамалық сигнал ұғымы машиналық нәтиженің аралық мәртебесін бекітуге, ал бес кезеңді модель дерек сапасын бақылауды, оқшауланған өңдеуді, адами верификацияны, құжаттауды және аудитті бір рәсімге біріктіруге мүмкіндік береді. Ведомстволық регламент, алдын ала әсерді бағалау, тыйым салынатын сценарийлер, екі сатылы тексеру және модельдер тізілімі іске асырылған жағдайда ЖИ ақпараттық талдаудың жылдамдығын арттырып қана қоймай, шешімнің заңдылығы мен есептілігін күшейтетін басқарылатын құрал бола алады.

Әдебиеттер тізімі:

1. Жедел-іздестіру қызметі туралы: Қазақстан Республикасының 1994 жылғы 15 қыркүйектегі № 154-XIII Заңы. Әділет ақпараттық-құқықтық жүйесі. https://adilet.zan.kz/kaz/docs/Z940004000_ (қаралған күні: 09.09.2026).

2. Жасанды интеллект туралы: Қазақстан Республикасының 2025 жылғы 17 қарашадағы № 230-VIII ҚРЗ Заңы. Әділет ақпараттық-құқықтық жүйесі. https://adilet.zan.kz/kaz/docs/Z2500000230 (қаралған күні: 09.09.2026).

3. Дербес деректер және оларды қорғау туралы: Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы. Әділет ақпараттық-құқықтық жүйесі. https://adilet.zan.kz/kaz/docs/Z1300000094 (қаралған күні: 09.09.2026).

4. Жасанды интеллектті дамытудың 2024-2029 жылдарға арналған тұжырымдамасын бекіту туралы: Қазақстан Республикасы Үкіметінің 2024 жылғы 24 шілдедегі № 592 қаулысы. https://adilet.zan.kz/kaz/docs/P2400000592 (қаралған күні: 09.09.2026).

5. UNICRI, INTERPOL. Toolkit for Responsible AI Innovation in Law Enforcement: Introduction to Responsible AI Innovation. Revised February 2024. https://unicri.org/sites/default/files/2024-02/01_Intro_Resp_AI_Innovation_Feb24.pdf (accessed: 09.09.2026).

6. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: National Institute of Standards and Technology, 2023. https://doi.org/10.6028/NIST.AI.100-1.

7. Autio C., Schwartz R., Dunietz J., Jain S., Stanley M., Tabassi E., Hall P., Roberts K. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. Gaithersburg: National Institute of Standards and Technology, 2024. https://doi.org/10.6028/NIST.AI.600-1.

8. Lum K., Isaac W. To predict and serve? Significance. 2016. Vol. 13, No. 5. P. 14-19. https://doi.org/10.1111/j.1740-9713.2016.00960.x.

9. Brayne S. Big Data Surveillance: The Case of Policing. American Sociological Review. 2017. Vol. 82, No. 5. P. 977-1008. https://doi.org/10.1177/0003122417725865.

10. Richardson R., Schultz J. M., Crawford K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online. 2019. Vol. 94. P. 192-233. https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf.

11. Oswald M., Grace J., Urwin S., Barnes G. C. Algorithmic risk assessment policing models: lessons from the Durham HART model and experimental proportionality. Information and Communications Technology Law. 2018. Vol. 27, No. 2. P. 223-250. https://doi.org/10.1080/13600834.2018.1458455.

12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Consolidated version of 27 July 2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng (accessed: 09.09.2026).

ЖАРЫЛКАСЫНОВ КУАНЫШ ӘБІЛҚАСЫМҰЛЫ
докторант 2 курса Академии управления
МВД Республики Казахстан
магистр юридических наук, капитан полиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЕ КАЗАХСТАНА: МОДЕЛИ, НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ

Развитие технологий искусственного интеллекта становится одним из ключевых направлений цифровой трансформации государственного управления и правоохранительной деятельности.

Данный процесс в последние годы приобретает практический характер: наряду с развитием информационных систем постепенно внедряются технологии интеллектуального анализа данных, распознавания лиц, прогнозирования преступности и автоматизации отдельных процессов расследования, цифровые решения начинают использоваться не только для обработки информации, но и для поддержки принятия решений.

В связи с этим возникает необходимость исследовать, насколько последовательно происходит переход от традиционной цифровизации к использованию искусственного интеллекта в правоохранительной системе Казахстана.

Целью настоящего исследования является анализ основных этапов и современных направлений внедрения технологий искусственного интеллекта в правоохранительную деятельность Казахстана, а также оценка достигнутых практических результатов и существующих проблем.

Особое внимание уделяется конкретным цифровым проектам, официальным статистическим данным и зарубежному опыту.

В исследовании использован комплексный методологический подход, который объединяет анализ научной литературы и технологический анализ. Обзор научных источников дал возможность выстроить теоретическую основу работы, выделить ключевые аспекты и обозначить основные направления развития искусственного интеллекта в правоохранительной деятельности.

Изучение литературы помогло получить представление о современном состоянии применения ИИ в этой сфере. Технологический анализ имеющихся решений и инструментов подтвердил их значение и пригодность для совершенствования процессов правоприменения. Указанные методы позволили оценить фактические результаты внедрения искусственного интеллекта. В совокупности комплексный подход обеспечил всестороннюю оценку потенциала ИИ в правоохранительной деятельности.

Начальный этап внедрения искусственного интеллекта в правоохранительную деятельность связывается с интеграцией технологий ИИ в Единый реестр досудебных расследований.

Цель внедрения заключается в повышении качества и ускорении расследования уголовных дел. Искусственный интеллект интегрирован в информационную систему «Единый реестр досудебных расследований» и

обеспечивает автоматизацию рутинных операций следователя. Система выполняет перевод устной речи в текст, сопоставление показаний с выявлением противоречий, формирование предложений по уточняющим вопросам при допросах, а также автоматическое составление процессуальных документов.

Обученная модель включает четыре модуля: планирование расследования, обработка показаний, подготовка документов, аналитика и прогнозирование. Применение данной технологии позволяет сократить сроки расследования и освободить следователей от значительной части технической работы. (1)

Кроме того, как отмечает А.Т. Темиржанов, искусственный интеллект способен оказать помощь в выявлении нарушений законодательства и условий, способствующих преступлениям, в подготовке шаблона представления с указанием адресата, а также в формулировании рекомендаций для включения в документ. По мнению автора, применение ИИ может способствовать продвижению идей законности и правопорядка, повышению правосознания граждан и укреплению доверия к государственным институтам. (2)

В аналитическом обзоре Казахстанского института стратегических исследований при Президенте РК А. Абдрашитова и Н. Затилла рассматривают практику внедрения цифровых технологий и искусственного интеллекта в правоохранительную систему Казахстана. Особое внимание уделяется опыту Генеральной прокуратуры, включая подходы к прогнозированию преступности, мониторингу обращений граждан и профилактике правонарушений. Авторы проводят сравнительный анализ цифровизации правоохранительных систем стран ОЭСР, Европейского союза и США, что позволяет сопоставить национальные решения с международными тенденциями. Отдельный раздел посвящён перспективам более глубокого применения ИИ, связанным с этим рискам и необходимости соблюдения баланса между эффективностью и защитой прав граждан. (3)

В Генеральной прокуратуре представлены два инновационных инструмента — «Crypto Trace» и «ProkAi», разработанные прокуратурой города Шымкент совместно с отечественными IT-компаниями для противодействия наркопреступности. Проекты реализованы на безвозмездной основе в рамках продвижения идеологемы «Закон и Порядок» и переданы на баланс прокуратуры. «Crypto Trace» представляет собой поисковую систему, предназначенную для анализа сетевых транзакций и выявления финансовых потоков наркобизнеса. «ProkAi» — интеллектуальная платформа, выявляющая торговлю наркотиками в интернете. Система функционирует круглосуточно и выполняет значительно больший объём поисковых операций по сравнению со специалистом. За три месяца работы чат-бота «ProkAi» установлено свыше 2 000 дропперских счетов. С использованием изъятых SimBox-устройств обеспечивается подключение к большому числу номеров наркомагазинов. Инструменты прошли апробацию в реальном расследовании: выявлено более 15 тыс. счетов дропперов (около 2 тыс. казахстанских, свыше 13 тыс. зарубежных и 620 криптовалютных), более ста лиц привлечены к уголовной ответственности. Удалось установить криптокошельки конечных выгодоприобретателей с активами около 5 млн USDT. Разработанные программы планируется внедрить по всей стране. (4)

С точки зрение перспективы приминение ИИ в деятельности правоохраительной очень расширенна и масштабна начина от досудебного производства и ОРД. Стоит также отметить о том, что в настоящее время НПА не регулируется приминение ИИ, что временами бывает проблемы как в теорическом плане так и практическом.

Интеграция цифровых интеллектуальных систем в правоохранительный сегмент охватывает широкий спектр задач, распространяясь как на стадию досудебного расследования, так и на оперативно-розыскное обеспечение. Однако отсутствие нормативного закрепления условий и пределов использования подобных технологий порождает научно-теоретическую неопределённость и создает правоприменительные риски.

Широкое проникновение информационно-аналитических технологий в различные институты общества предопределяет их высокий потенциал и при выполнении задач правоохранительной направленности. В рамках раскрытия преступлений и сбора доказательственного материала должностные лица органов досудебного расследования регулярно сталкиваются с необходимостью обработки масштабных массивов сведений, служащих основой для выдвижения криминалистических версий и планирования следственных действий. В связи с этим закономерно актуализируется вопрос об интеграции современных технологических разработок, включая системы искусственного интеллекта, в деятельность по оптимизации и повышению оперативности работы с поступающими процессуальными и оперативно-разыскными данными. (5)

Анализ практики применения специализированных алгоритмических систем в зарубежных правоохранительных и судебных органах демонстрирует существенные риски проявления дискриминационных сдвигов (алгоритмической предвзятости) и фактических ошибок. В частности, независимое исследование алгоритма COMPAS, используемого для прогнозирования вероятности рецидива, выявило его общую низкую прогностическую точность: при предсказании вероятности повторного совершения насильственных преступлений корректность оценок составила лишь 20%.

Более того, логистическая регрессия показала системные искажения при оценке факторов риска: темнокожие обвиняемые, не совершавшие впоследствии правонарушений, относились к категории высокого риска почти вдвое чаще по сравнению с белыми гражданами (45% против 23%), в то время как среди белых рецидивистов 48% ошибочно квалифицировались системой как лица с низким уровнем опасности [6].

Данные результаты подтверждают, что математическое моделирование криминологических рисков без надлежащего процессуального контроля способно воспроизводить и усиливать существующие дефекты правоприменительной практики.

Систематизируя условия эффективной цифровизации оперативно-разыскной деятельности в Республике Казахстан, Беркишев Е.О. выделяет комплекс взаимосвязанных институциональных и правовых мер. По мнению исследователей, успешная интеграция интеллектуальных систем в указанную сферу требует:

- обстоятельного анализа и адаптации передового зарубежного опыта с учётом специфики национального законодательства и правоприменительной практики;
- формирования специализированной нормативной правовой базы, регламентирующей порядок и пределы использования технологий искусственного интеллекта при проведении оперативно-разыскных мероприятий;
- нормативного обеспечения алгоритмической транспарентности и поднадзорности цифровых решений, а также создания процессуальных гарантий защиты прав граждан от дискриминации и злоупотреблений;
- организации непрерывной профессиональной подготовки и повышения квалификации сотрудников правоохранительных органов в сфере прикладного применения информационных систем;
- выстраивания межведомственного и междисциплинарного взаимодействия между научно-исследовательскими организациями, IT-сектором и правоохранительными структурами.

Реализация данных шагов призвана обеспечить баланс между повышением результативности выявления и раскрытия правонарушений и неукоснительным соблюдением конституционных прав и свобод личности. [7].

Формирование национальной стратегии цифровизации правосудия рассматривается в качестве обязательного условия системного освоения инновационных технологий судебными органами Казахстана. В исследовании Н. Т. Байтилесова подчеркивается, что соответствующий стратегический документ должен предусматривать комплексную реализацию следующих направлений:

- создание единой электронно-цифровой среды судебной системы;
- введение обязательной государственной сертификации алгоритмов и программных решений, применяемых в судопроизводстве;
- организация специализированного обучения судейского корпуса и работников аппаратов судов вопросам этики использования цифровых инструментов и предупреждения алгоритмической предвзятости;
- локализация процессов хранения и обработки судебной информации на отечественных облачных платформах с обеспечением национальных стандартов криптографической защиты данных;
- учреждение национального реестра сбоев и ошибок алгоритмических систем для оперативного реагирования на дефекты в их функционировании [8].

Проведённое исследование показывает, что внедрение искусственного интеллекта в правоохранительную систему Казахстана перешло от единичных инициатив к системной практике, охватывающей досудебное расследование, деятельность прокуратуры и перспективы цифровизации правосудия.

Интеграция ИИ в «Единый реестр досудебных расследований» позволила автоматизировать распознавание речи, сопоставление показаний и подготовку процессуальных документов, освободив следователей от рутинных операций. Инструменты прокуратуры «Crypto Trace» и «ProkAi» продемонстрировали высокую эффективность в противодействии наркопреступности, выявив тысячи дропперских счетов и криптокошельков. Это подтверждает практическую пользу цифровых решений для правоохранительной деятельности.

Одновременно выявлены проблемы. Зарубежный опыт применения алгоритма COMPAS показал риск алгоритмической предвзятости и ошибок при прогнозировании рецидива, что требует обязательного процессуального контроля со стороны человека. Кроме того, в Казахстане отсутствует специальное нормативное регулирование применения ИИ в правоохранительной сфере, что порождает теоретическую и практическую неопределённость.

Решение этих проблем исследователи связывают с формированием соответствующей правовой базы: адаптацией зарубежного опыта, закреплением пределов использования ИИ в нормативных актах, обеспечением алгоритмической прозрачности и подконтрольности, подготовкой кадров и межведомственным взаимодействием. Применительно к судебной системе предлагается разработка национальной стратегии цифровизации, включающей сертификацию алгоритмов, обучение судей, локализацию данных и учёт сбоев систем.

Таким образом, практическая значимость результатов заключается в подтверждении работоспособности технологий ИИ в казахстанской правоохранительной практике при одновременной необходимости опережающего правового регулирования. Дальнейшее развитие данного направления требует сочетания расширения апробированных цифровых решений с созданием нормативной базы, гарантирующей защиту прав граждан и подконтрольность алгоритмических систем.

Список литературы:

1. Искусственный интеллект помогает следствию [Электронный ресурс] // Официальный интернет-ресурс государственных органов Республики Казахстан. – URL: https://www.gov.kz/memleket/entities/qriim/press/news/details/1021249?lang=ru (дата обращения: 27.08.2026).
2. Темиржанов А.Т. О проводимой работе по внедрению искусственного интеллекта // Сборник материалов Международной научно-практической конференции «Право в условиях глобальной трансформации: современные вызовы и перспективы развития». 08.04.2026. С. 106–109.
3. Прокуроры Казахстана разработали ИИ-помощника для анализа уголовных дел [Электронный ресурс] // Kazakhstan Today. – 05.08.2026. – URL: https://www.kt.kz/rus/state/prokurory_kazahstana_razrabotali_ii_dlya_analiza_ugolovnyh_1377996492.html (дата обращения: 27.08.2026).
4. В Генеральной прокуратуре презентованы инновационные инструменты «Crypto Trace» и «ProkAi» [Электронный ресурс] // Официальный интернет-ресурс государственных органов Республики Казахстан. – URL: https://www.gov.kz/memleket/entities/sko-airtau/press/news/details/1102105?lang=ru (дата обращения: 27.08.2026)
5. Шурдумов А. А. Искусственный интеллект как криминалистический инструмент // Теория и практика общественного развития. 2025. № 6. С. 273–278. DOI: 10.24158/tipor.2025.6.34.
6. Larson J., Mattu S., Kirchner L., Angwin J. How We Analyzed the COMPAS Recidivism Algorithm // ProPublica. 2016.
7. Беркишев Е. О. Зарубежный опыт применения искусственного интеллекта в оперативно-розыскной деятельности // Вестник Карагандинской академии МВД РК им. Баримбека Бейсенова. 2026. № 1 (91). С. 299–303.
8. Байтилесов Н. Т. К вопросу об интеграции этически ориентированного искусственного интеллекта в цифровое правосудие // Вестник Карагандинской академии МВД РК им. Баримбека Бейсенова. 2026. № 1 (91). С. 15. [1, с. 15].

ЖОЛШЫБАЙ ӘСЕМКҮЛ ҚУАНЫШҚЫЗЫ
Магистрант ЕНУ имени Л.Н. Гумилева
научно-педагогическое направление (2026-2028)
по специальности «Судебная экспертиза»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИССЛЕДОВАНИИ ФОТО- И ВИДЕОМАТЕРИАЛОВ: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ И КРИМИНАЛИСТИЧЕСКИЕ ЗАДАЧИ

Стремительная цифровизация общественной жизни коренным образом изменила структуру доказательственной базы в уголовном судопроизводстве. Сегодня ключевыми источниками доказательств всё чаще становятся фото- и видеоматериалы: записи камер наружного наблюдения, автомобильных регистраторов, контент из социальных сетей и мобильных устройств граждан. Но лавинообразный рост объёма визуальных данных создаёт серьёзные проблемы для следственных органов – традиционный визуальный осмотр медиафайлов силами одного эксперта становится попросту неэффективным из-за колоссальных временных затрат.

В этих условиях автоматизация экспертной деятельности через внедрение систем искусственного интеллекта (ИИ) и компьютерного зрения (Computer Vision) давно перешла из разряда перспективных концепций в плоскость повседневной криминалистической практики. Казахстанская судебно-экспертная школа активно реагирует на эти вызовы: как справедливо отмечают профессора С.Ф. Бычкова и К.К. Сейтенов, научно-методические основы судебной экспертизы должны непрерывно адаптироваться под технологическое состояние правоприменительной практики [1; 2].

Показательно, что речь идёт не только о теории. По данным на 2025 год в Казахстане действует свыше 1,6 млн камер видеонаблюдения, значительная часть которых оснащена элементами ИИ; около 90 тыс. камер подключено к центрам оперативного управления полиции, а порядка 27 тыс. из них способны самостоятельно анализировать видеопоток – в первую очередь в целях обеспечения дорожной безопасности [3]. Параллельно Генеральная прокуратура РК совместно с МВД РК реализует проекты по интеграции ИИ в процесс досудебного расследования, а на базе информационно-аналитической платформы Smart Data Ukimet, аккумулирующей данные из 93 государственных и квазигосударственных баз, отрабатываются механизмы комплексного анализа больших массивов данных [3]. Это делает теоретическое осмысление возможностей нейросетей в исследовании медиаданных не абстрактным, а вполне прикладным вопросом.

Современные возможности ИИ при анализе фото- и видеоматериалов

Применение алгоритмов машинного обучения в криминалистическом исследовании изображений и видеопотоков развивается сегодня по нескольким основным направлениям. Системы ИИ способны одновременно обрабатывать визуальный, звуковой и текстовый слои информации, выявляя закономерности, которые человек-эксперт при ручном просмотре, скорее всего, пропустит.

1. Биометрическая идентификация и распознавание лиц. Нейросетевые модели глубокого обучения автоматизируют сопоставление лиц на видеозаписях низкого качества с базами разыскиваемых лиц. Такие технологии достаточно устойчивы к смене ракурса, естественному старению человека, изменению причёски или наличию элементов маскировки – очков, бороды, медицинской маски.

2. Интеллектуальный анализ видеопотока и детекция объектов. ИИ избавляет эксперта от рутинного отсмотра многочасовых архивов: алгоритмы способны за секунды отфильтровать нужные фрагменты по заданным триггерам – марка и номер автомобиля, наличие в кадре оружия, особенности одежды человека или траектория его перемещения.

3. Улучшение качества и реконструкция изображений. Генеративно-состязательные сети (GAN) позволяют частично компенсировать артефакты сжатия, цифровой шум и смазанность кадра, возникшие из-за быстрого движения объекта или недостатка освещения.

Внедрение этих инструментов в Казахстане уже показывает практическую отдачу. Помимо упомянутой Smart Data Ukimet, отдельного внимания заслуживает и то, что подобные разработки ведутся не только на уровне государственных платформ, но и в академической среде – так, в рамках Nazarbayev University проводились экспериментальные работы по объединению нескольких сверточных архитектур (Xception, DenseNet-121, ResNet, MesoNet) для повышения точности распознавания подделанных изображений лиц, что говорит о формировании отечественной исследовательской базы в этой области [7].

Классификация криминалистических задач, решаемых с помощью ИИ

Интеграция ИИ в процесс исследования фото- и видеоматериалов позволяет достаточно чётко разделить следственные задачи на диагностические и идентификационные. На эту классификацию как методологическую основу экспертной деятельности неоднократно указывал в своих трудах профессор А.Ф. Аубакиров [4].

Диагностические задачи направлены на установление пространственно-временных обстоятельств события и выявление признаков модификации файлов. Нейросети успешно определяют примерное время фиксации по направлению и длине теней, реконструируют геопозицию по деталям ландшафта, а также выявляют факты вмешательства в структуру файла – склейки, удаление кадров, повторное пережатие.

Идентификационные задачи связаны с установлением конкретного тождества. Сюда относится не только классическое распознавание личности, но и идентификация технических средств, на которые производилась съёмка. В частности, ИИ способен анализировать специфический паттерн шума матрицы видеокамеры (PRNU – Photo Response Non-Uniformity), который из-за микроскопических дефектов изготовления сенсора уникален для каждого конкретного устройства и работает как своего рода «цифровой отпечаток пальца» камеры.

Проблема дипфейков как новый экспертный вызов

Обратная сторона технологического прогресса – использование ИИ криминальными элементами. Распространение технологий генерации

высококачественных подделок (deepfake) поставило под сомнение сам статус видеозаписи как достоверного доказательства. Как отмечает Б.Г. Нургалиев, появление цифровых способов фальсификации требует создания принципиально новых криминалистических алгоритмов противодействия [5].

Подделка биометрических данных лица или синтез чужого голоса сегодня вполне может стать орудием мошенничества, шантажа или создания ложного алиби. Перед казахстанскими криминалистами встаёт новая задача – разработка экспертных методик верификации достоверности цифрового контента.

Алгоритмы обнаружения фальсификаций анализируют микронесоответствия, незаметные для человеческого глаза: аномалии в частоте моргания, неестественные границы светотени на стыке кожи и фона, несоответствие едва уловимой пульсации кровеносных сосудов лица общей картине, а также спектральные искажения звуковой дорожки. Наиболее известным полигоном для отработки подобных детекторов остаётся набор данных FaceForensics++, объединяющий свыше 1,8 млн изображений, полученных четырьмя разными методами подделки лица (Deepfakes, Face2Face, FaceSwap, NeuralTextures). Классические архитектуры вроде XceptionNet показывают на нём точность свыше 99%, если модель обучалась и тестировалась на одном и том же способе подделки, – однако при переносе на незнакомый метод генерации или другой набор данных точность заметно падает. Это в точности повторяет проблему, характерную и для аудио-детекторов deepfake: высокий результат на «своём» наборе данных не гарантирует надёжной работы в реальных, заранее не предусмотренных условиях [6].

В Казахстане данное направление пока только формируется в рамках судебной компьютерно-технической и фототехнической экспертизы, и без отечественных исследовательских наборов данных – с учётом типичных для местной практики условий съёмки, сжатия и передачи файлов – оценить реальную применимость зарубежных детекторов будет затруднительно.

Процессуальные и этические риски использования ИИ

Несмотря на высокую технологическую точность, ИИ не может полностью заменить эксперта-криминалиста. В казахстанской доктрине, сформулированной профессором С.Ф. Бычковой, судебная экспертиза жёстко регламентирована принципами законности, научной обоснованности и проверяемости методов [1]. В связи с этим применение систем ИИ наталкивается на ряд серьёзных ограничений.

1. Проблема «чёрного ящика». Большинство современных нейросетей выдают вероятностный результат, но не могут объяснить логику его формирования в понятных человеку терминах. Криминалистическое заключение же должно быть прозрачным и проверяемым для суда – эксперт не может обосновать вывод фразой «так решила программа». Отсюда вытекает практическое требование: в заключении необходимо фиксировать не только итоговую оценку, но и то, на каком наборе данных обучалась и валидировалась модель, какова её точность на независимых выборках и в каких условиях (качество съёмки, метод подделки, степень сжатия) эта точность подтверждена – иначе результат работы алгоритма рискует быть представлен суду как категоричный факт, которым он на самом деле не является.

2. Юридическая ответственность. Системы ИИ выступают исключительно в роли интеллектуального ассистента специалиста. Всю процессуальную ответственность за итоговое заключение несёт конкретный судебный эксперт, подписывающий документ в порядке, установленном уголовно-процессуальным законодательством РК.

3. Риск предвзятости данных. Алгоритмы обучаются на готовых массивах информации, и если обучающая выборка содержала системные ошибки, искажения или была недостаточно репрезентативна – например, в части типичных для Казахстана условий съёмки и качества видеопотока, ИИ неизбежно продублирует эти недостатки уже в практической деятельности.

Заключение

Искусственный интеллект существенно расширил возможности криминалистического анализа фото- и видеоматериалов, сократив время обработки цифровых улик с недель до считанных минут. Опыт Генеральной прокуратуры и МВД Республики Казахстан подтверждает, что развитие следственных действий сегодня во многом связано с их алгоритмизацией.

Вместе с тем полноценная интеграция ИИ в правовое поле требует неукоснительного соблюдения методологических стандартов, заложенных отечественной школой судебной экспертологии, а применительно к задаче выявления дипфейков – создания собственных, проверенных на местном материале наборов данных и методик оценки надёжности детекторов. Технологии ИИ должны оставаться строго подконтрольным инструментом в руках человека, обеспечивая неотвратимость наказания при безусловном соблюдении законности и прав граждан.

Список литературы:

1. Бычкова С.Ф. Судебная экспертиза в уголовном судопроизводстве Республики Казахстан: теория и практика организации. – Алматы: Жеті жарғы, 2002. – 416 с.

2. Сейтенов К.К. Развитие судебной экспертизы в Республике Казахстан в условиях цифровизации уголовного процесса // Вестник Института законодательства и правовой информации РК. – 2021. -№ 3 (66). – С. 112-119.

3. Официальный сайт Генеральной Прокуратуры Республики Казахстан. Инновационные подходы и применение технологий искусственного интеллекта в надзорной деятельности и досудебном расследовании. [Электронный ресурс]. URL: gov.kz (дата обращения: 2026).

4. Аубакиров А.Ф. Криминалистическая классификация задач судебной фототехнической и видеотехнической экспертизы // Труды «Джакишевских чтений»: Материалы международной научно-практической конференции. — Алматы: КазНУ им. аль-Фараби, 2018. -С. 45-51.

5. Нургалиев Б.Г., Лакбаев К.С. Цифровые следы в криминалистике: теоретико-методологические проблемы исследования электронных носителей информации // Карагандинский вестник МВД РК. – 2020. – № 2. – С. 78-84.

6. Rössler A., Cozzolino D., Verdoliva L., Riess C., Thies J., Nießner M. FaceForensics++: Learning to Detect Manipulated Facial Images // Proceedings of the IEEE/CVF International Conference on Computer Vision. – 2019.

7. Nurgozhin T. Deepfake Detection via Feature-Level Fusion of Convolutional Neural Networks. – Nazarbayev University School of Engineering and Digital Sciences, 2025.

ЖУМАБАЕВ МЕЙРАМ АЗАМАТОВИЧ
ОФ «Esbol Qory» – менеджер проектов,
правовед

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: ТЕОРИЯ, ЗАКОНОДАТЕЛЬСТВО И ПРАВОПРИМЕНИТЕЛЬНАЯ ПРАКТИКА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Введение

Современный этап развития общества и государства неразрывно связан с глобальной цифровизацией всех сфер жизнедеятельности, что закономерно влечет за собой глубокую и качественную трансформацию преступности. Классические формы криминальных проявлений, традиционно опиравшиеся на физическое присутствие и прямой умысел в материальном мире, стремительно уступают место высокотехнологичным, дистанционным и транснациональным способам совершения правонарушений. В этих условиях устоявшаяся модель оперативно-розыскной деятельности (ОРД), которая формировалась преимущественно в доцифровую эпоху, сталкивается с беспрецедентными вызовами. Данные вызовы требуют не точечных корректировок, а глубокого, системного переосмысления фундаментальных основы ОРД как на теоретическом, так и на законодательном уровне.

Одной из наиболее острых проблем современности, представляющей прямую угрозу национальной безопасности, является стремительное распространение синтетических наркотических средств и массированное вовлечение в этот деструктивный процесс молодежи. Преступные синдикаты адаптировали корпоративные IT-модели управления под свои нужды, создав децентрализованные сети сбыта. Если ранее классические схемы наркоторговли выстраивались на физическом контакте «из рук в руки», что делало их уязвимыми для стандартных методов наружного наблюдения и контрольного закупа, то сегодня весь операционный цикл переведен в цифровое пространство. От агрессивной вербовки низовых курьеров до сложнейших схем легализации доходов через криптовалютные транзакции – все процессы осуществляются через теневой сегмент сети Интернет (DarkNet), специализированные форумы и защищенные мессенджеры со сквозным шифрованием. Подобная криминальная эволюция ставит перед подразделениями криминальной полиции и органами национальной безопасности принципиально новые, интеллектуально емкие задачи, успешное решение которых априори невозможно без концептуальной модернизации всего инструментария ОРД.

1. Гносеологические и теоретические основы ОРД в киберпространстве

С теоретической и методологической точек зрения фундаментальные основы оперативно-розыскной деятельности остро нуждаются в расширении и актуализации понятийного аппарата. Существующая доктрина отечественной ОРД исторически базируется на приоритете физического пространства. Законодатель и правоприменитель традиционно исходят из необходимости непосредственного

контакта оперативного сотрудника с объектом оперативной разработки, местом происшествия или негласным источником информации. Однако в реалиях информационного общества и всеобъемлющей «цифровой анонимности» объектом первичного оперативного интереса все чаще выступает не идентифицированное физическое лицо, а оставленный им «цифровой след».

Цифровой след в контексте криминальной аналитики представляет собой сложный массив данных: сетевые псевдонимы (аккаунты), динамические и статические IP-адреса, уникальные идентификаторы мобильных устройств (IMEI, MAC-адреса), адреса криптовалютных кошельков, а также специфические поведенческие паттерны пользователя в сети. В этой связи в теории ОРД возникает закономерный и до сих пор не разрешенный дискуссионный вопрос: как именно с правовой точки зрения квалифицировать действия оперативного сотрудника, осуществляющего поиск и фиксацию информации исключительно в виртуальной среде?

Является ли, к примеру, углубленный мониторинг открытых источников с применением методологии OSINT (Open-Source Intelligence) или агрегированный анализ больших данных (Big Data) самостоятельным оперативно-розыскным мероприятием (ОРМ)? Или же это следует трактовать лишь как современный технический способ наведения справок и фиксации информации?

На сегодняшний день консервативная теория ОРД не предоставляет исчерпывающих ответов на эти вопросы. Отсутствие доктринальной ясности неминуемо проецируется на практику, порождая процессуальную неопределенность, при которой результаты сложнейшей оперативно-аналитической работы рискуют быть признанными недопустимыми доказательствами на стадии судебного следствия из-за нарушения формы их собирания.

Происходит кардинальная трансформация роли самого субъекта ОРД. Оперативный сотрудник эволюционирует из классического «добытчика» информации в «аналитика-интегратора». Если ранее ключевым навыком являлось умение установить психологический контакт с информаторами или грамотно организовать засаду, то современный специалист должен обладать навыками сопоставления разрозненных фрагментов цифровых данных, дешифровки потоков информации и понимания архитектуры сетевых протоколов. Игнорирование этого сдвига в парадигме оперативного познания ведет к стагнации всей правоохранительной системы.

2. Эволюция наркопреступности: от физического контакта к теневым сетям

Анализируя трансформацию преступной среды, необходимо детально остановиться на феномене бесконтактного сбыта синтетических наркотиков. Данный вид преступного промысла стал своеобразным полигоном для обкатки самых передовых IT-решений криминалитетом. Архитектура современного интернет-магазина по продаже наркотиков представляет собой многоуровневую, строго иерархичную корпорацию с четким разделением труда, где ни одно из звеньев физически не взаимодействует с другими.

Организаторы, находящиеся, как правило, за пределами национальной юрисдикции, управляют процессом посредством защищенных серверов.

Финансовые потоки контролируются автоматизированными Telegram-ботами и проходят стадию многократного дробления через криптовалютные миксеры, что делает невозможным их прямое отслеживание традиционными методами финансового мониторинга. «Вербовщики» используют методы агрессивного маркетинга и социальной инженерии, таргетируя рекламу легкого заработка на уязвимые слои населения, в первую очередь – на студентов и школьников.

В таких условиях задержание низового звена – рядовых закладчиков, на которых зачастую ориентирована отчетность региональных подразделений, – не оказывает абсолютно никакого влияния на жизнеспособность самого наркосиндиката. Для организаторов бизнеса арестованный закладчик является лишь расходным материалом, чье место в течение нескольких суток занимает новый рекрут. Эта конвейерная система бесперебойно работает именно благодаря цифровой изоляции каждого участника преступной схемы.

3. Критический анализ устаревших методов: отказ от выявления и проверки интернет-ссылок

Пересмотр методологии противодействия цифровой преступности требует жесткого аудита текущих оперативных практик. Ключевым императивом на современном этапе является объективная необходимость убрать мероприятия, направленные на механическое выявление и проверку ссылок. Многолетняя практика мониторинга открытого сегмента сети с целью ручной или полуавтоматической фиксации и последующей блокировки URL-адресов наркошопов доказала свою абсолютную оперативно-стратегическую несостоятельность.

В условиях, когда криминальные IT-специалисты применяют скрипты автоматической генерации «зеркал», используют динамическую маршрутизацию и легко заменяемые Telegram-боты, блокировка конкретного адреса или ссылки ограничивает доступ к ресурсу лишь на считанные минуты. Затраты времени и человеческих ресурсов сотрудников правоохранительных органов на оформление процессуальных документов для блокировки совершенно не сопоставимы с теми секундами, которые требуются алгоритму преступников для развертывания новой ссылки.

Данная деятельность представляет собой классический Сизифов труд, создающий видимость активной борьбы, но не наносящий урона ядру преступной группы. ОРД должна категорически сместить вектор внимания с борьбы со следствиями (блокировки ссылок) на ликвидацию первопричин. Основной удар должен быть направлен на выявление главных администраторов платформ, деанонимизацию теневых финансистов, перекрытие крупных каналов поставки прекурсоров и демонтаж серверной инфраструктуры преступных сообществ. Только переход от экстенсивных, «количественных» методов к интенсивной, глубокой цифровой аналитике способен переломить ситуацию.

4. Правовые и этические аспекты применения искусственного интеллекта в ОРД

Наиболее перспективным ответом на вызовы киберпреступности является интеграция технологий искусственного интеллекта (ИИ) и алгоритмов машинного обучения в арсенал оперативно-розыскной деятельности. Системы предиктивной

аналитики способны в фоновом режиме агрегировать терабайты неструктурированных данных из разнородных источников: биллингов операторов сотовой связи, транзакций финансовых учреждений, записей камер городского видеонаблюдения и открытых данных социальных сетей.

Нейросети, обученные на паттернах преступного поведения, могут с высокой долей вероятности выявлять аномалии, указывающие на подготовку к совершению преступления. Например, алгоритм может сопоставить регулярные микропереводы с различных банковских карт на один криптокошелек с геолокацией мобильных устройств в парковых зонах в ночное время, автоматически формируя сигнал тревоги (alert) для оперативного дежурного. Внедрение систем интеллектуального распознавания лиц и анализа видеопотока уже доказало свою эффективность в розыске преступников «по горячим следам».

Однако форсированное внедрение ИИ сопровождается комплексом серьезных правовых и этических дилемм. Во-первых, возникает так называемая проблема «черного ящика» (Black Box problem). Глубокие нейросети функционируют на основе многослойных матричных вычислений, логика которых зачастую непонятна даже самим разработчикам алгоритма. Если нейросеть указывает на причастность лица к наркосиндикату, следователю крайне сложно объяснить в суде, на основании каких конкретно критериев машина сделала такой вывод. Это вступает в прямое противоречие с уголовно-процессуальными принципами проверяемости и достоверности доказательств.

Во-вторых, сохраняется высокий риск алгоритмической предвзятости. Если исторические данные, на которых обучалась модель прогнозирования преступности, содержали искажения (например, усиленное патрулирование определенных районов), ИИ будет реплицировать эти ошибки, направляя полицейские силы на те же участки, что приведет к гипертрофированному контролю и нарушению прав граждан. В связи с этим, внедрение ИИ должно строго подчиняться принципу «человек в контуре» (Human-in-the-loop): алгоритм является лишь инструментом аналитической поддержки, а правовая оценка, принятие процессуального решения и бремя юридической ответственности всегда и всецело лежат на должностном лице.

5. Проблемы процессуальной легализации цифровых данных и взаимодействие с финансовым сектором

Переходя к законодательному аспекту, следует констатировать, что Закон Республики Казахстан «Об оперативно-розыскной деятельности», несмотря на вносимые поправки, концептуально остается в фарватере доцифровой эпохи. Закрепленный в законе перечень оперативно-розыскных мероприятий (ОРМ) ориентирован на аналоговые методы. Острая нехватка специализированных норм, детально регламентирующих изъятие виртуальных активов, снятие дампов памяти облачных серверов или проведение негласного обследования в сети Интернет (кибер-патрулирования), создает зону правовой неопределенности.

Отсутствие четкой регламентации порядка применения специальных программных комплексов для деанонимизации пользователей или перехвата зашифрованного трафика несет в себе риски необоснованного ограничения конституционных прав граждан на тайну переписки и неприкосновенность частной

жизни. Любое сомнение в законности получения информации трактуется судом в пользу обвиняемого, что приводит к признанию важнейших электронных носителей недопустимыми доказательствами. Решение данной проблемы видится в разработке детализированных инструкций по легализации электронных доказательств, обеспечении их целостности посредством хеширования (например, алгоритмами SHA-256) на этапе первичного изъятия.

Важнейшим рубежом борьбы с организованной преступностью выступает финансовый сектор. Значительная часть оперативно значимой информации (транзакции, IP-адреса входов в банковские приложения, идентификация P2P-переводов) аккумулируется в базах данных банков второго уровня и операторов фискальных данных. Существующий порядок взаимодействия правоохранительных органов с частным сектором чрезмерно забюрократизирован. Процедура санкционирования запросов и ожидания ответов может занимать от нескольких дней до недель, тогда как движение криминальных средств через криптобиржи происходит за доли секунды. Требуется внедрение защищенных шлюзов для автоматизированного, мгновенного обмена электронными документами между субъектами ОРД и финансовыми институтами с соблюдением требований информационной безопасности.

Не менее остро стоит проблема кадрового голода. Правоохранительная система испытывает острый дефицит «кибер-следователей» и оперативных сотрудников с профильным IT-образованием. Преодоление этого разрыва требует отказа от формального подхода к переподготовке кадров в ведомственных академиях. Необходимо привлекать гражданских IT-специалистов на контрактой основе, обучать действующих сотрудников основам криптоанализа, OSINT-разведки и программирования на скриптовых языках для самостоятельной обработки массивов данных.

6. Предложения для руководства Министерства внутренних дел Республики Казахстан

В целях концептуальной модернизации оперативно-розыскной деятельности, приведения ее методологического арсенала в соответствие с вызовами цифровой эпохи и повышения эффективности противодействия организованной транснациональной преступности, предлагается следующий комплекс неотложных мер:

- Официально закрепить использование методов «исследования открытых компьютерных сетей (OSINT)» как современного технического способа в рамках уже существующих ОРМ (например, оперативного поиска или наведения справок), а также регламентировать «негласный мониторинг цифровых транзакций», исключив произвольное вмешательство в частную жизнь граждан.
- Разработать и внедрить защищенный программный интерфейс (API) для регламентного, юридически значимого и ускоренного получения оперативно-значимой информации от банков второго уровня, провайдеров хостинга и операторов сотовой связи, интегрированный с модулем электронного санкционирования (например, через систему «Е-Уголовное дело»). Интеграция должна обеспечивать мгновенный обмен данными исключительно после получения

соответствующей санкции в рамках расследования тяжких и особо тяжких преступлений.

- Инициировать изменения в Закон РК «О правоохранительной службе» для создания специальных должностей «кибер-аналитиков» с особым порядком прохождения службы (без учета строевых и физических нормативов)».

Заключение

Резюмируя проведенный анализ, следует констатировать, что актуальные проблемы оперативно-розыскной деятельности носят глубокий системный характер. Адекватный ответ на вызовы цифровой эпохи невозможен путем косметических изменений нормативной базы или закупки отдельного программного обеспечения. Требуется комплексный, стратегический подход, охватывающий модернизацию доктринальной теории, обновление уголовно-процессуального законодательства и полную трансформацию методов практической работы «на земле» и в киберпространстве. Только синергия передовых аналитических технологий, выверенной, защищающей права человека нормативной базы и высокого профессионализма сотрудников способна обеспечить надежный правоохранительный щит против современной организованной преступности, гарантируя национальную безопасность Республики Казахстан в условиях глобальной цифровизации.

Список литературы:

1. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 г.).
2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V.
3. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V.
4. Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности».
5. Смирнов М.П. Комментарий к закону об оперативно-розыскной деятельности. Теория и практика. – М., 2021.
6. Овчинский В.С. Криминология цифрового мира. – М.: Норма, 2018.
7. Материалы судебной практики Верховного Суда Республики Казахстан по делам о незаконном обороте наркотических средств с использованием информационно-коммуникационных технологий.
8. Чекотков А.В. Теоретико-правовые основы использования цифровых следов в расследовании преступлений // Вестник криминалистики. 2023. № 2. С. 45-52.
9. Иванов А.И. Искусственный интеллект в оперативно-розыскной деятельности: правовые границы и перспективы // Юридическая наука и практика. 2024. Т. 15. № 1. С. 112-120.

ЖУНИСБЕКОВ НУРКЕН НУРАХМЕТОВИЧ
Старший преподаватель кафедры
Оперативно-розыскной деятельности Карагандинской академии
МВД Республики Казахстан имени Б. Бейсенова
доктор философии (PhD), подполковник полиции

ПРАВОВЫЕ И ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ OSINT В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация.
Расширение цифрового пространства существенно изменило способы получения информации, представляющей интерес для правоохранительных органов. Одним из востребованных направлений становится разведка по открытым источникам (Open Source Intelligence, OSINT), позволяющая выявлять и анализировать сведения, размещенные в общедоступной информационной среде. В статье исследуются возможности применения OSINT в оперативно-розыскной деятельности Республики Казахстан с учетом действующих правовых ограничений. Рассматриваются основные категории открытых источников, условия правомерного получения сведений, вопросы защиты частной жизни и персональных данных. Отдельное внимание уделяется использованию результатов OSINT в уголовном процессе, их проверке, фиксации и обеспечению целостности цифровых материалов. Анализируются риски, связанные с распространением недостоверного и искусственно созданного контента, нарушением порядка хранения цифровой информации и отсутствием специального правового регулирования OSINT. Предлагаются направления совершенствования нормативных и организационно-методических основ использования открытых источников в деятельности правоохранительных органов.

Ключевые слова: *OSINT, оперативно-розыскная деятельность, открытые источники, цифровые доказательства, уголовный процесс, персональные данные.*

Введение

Развитие информационно-коммуникационных технологий привело не только к расширению возможностей обмена информацией, но и к изменению среды, в которой осуществляется противоправная деятельность. Значительная часть коммуникаций, подготовки отдельных преступлений и действий, направленных на сокрытие их следов, осуществляется с использованием социальных сетей, мессенджеров, форумов и других цифровых платформ. В подобных условиях сведения, доступные в сети Интернет, приобретают практическую ценность для оперативных подразделений. Одним из способов их систематизированного получения и анализа выступает разведка по открытым источникам — OSINT [1].

Под OSINT понимается целенаправленный поиск, сбор, обработка и аналитическая оценка информации, доступ к которой возможен без использования специальных технических средств негласного получения сведений [1]. Информационную основу такого поиска могут составлять публикации средств массовой информации, официальные интернет-ресурсы государственных органов,

социальные сети, блоги, форумы, видеохостинги, публичные базы данных и другие ресурсы открытого доступа. Анализ этих источников позволяет устанавливать информационные связи между объектами, исследовать публичную цифровую активность интересующих лиц, получать сведения ориентирующего характера и формировать версии для дальнейшей проверки оперативными и процессуальными средствами [1].

При этом в законодательстве Республики Казахстан OSINT не закреплен в качестве самостоятельной правовой категории. Закон Республики Казахстан «Об оперативно-розыскной деятельности» предусматривает возможность получения сведений, необходимых для выполнения задач ОРД, при обязательном соблюдении принципа законности и гарантированных прав граждан [2]. Содержание действующих норм позволяет использовать общедоступные сведения посредством наведения справок, изучения открытых информационных ресурсов и иных действий, не предполагающих неправомерного ограничения конституционных прав. Поэтому на практике OSINT может применяться в пределах существующих механизмов оперативно-розыскной деятельности, несмотря на отсутствие его отдельного нормативного определения [2].

Правовые границы использования открытых источников.

Общедоступность информации сама по себе не устраняет необходимость соблюдения правовых ограничений при ее получении и последующем использовании. Конституция Республики Казахстан гарантирует неприкосновенность частной жизни, личной и семейной тайны, а также защиту тайны переписки и иных сообщений [3]. В связи с этим принципиальное значение имеет способ доступа к информации.

Сведения могут рассматриваться в качестве полученных из открытого источника, если доступ к ним объективно не ограничен законом либо самим владельцем соответствующего информационного ресурса. Получение закрытой информации посредством неправомерного доступа к учетной записи, преодоления технических механизмов защиты или обращения к незаконно распространенным базам данных уже не соответствует содержанию OSINT. Подобные действия должны оцениваться с учетом самостоятельных требований законодательства [5].

Правовой режим информации тесно связан и с законодательством о персональных данных. Закон Республики Казахстан «О персональных данных и их защите» предусматривает возможность обработки общедоступных персональных данных, одновременно устанавливая ограничения в отношении сведений, доступ к которым ограничен [5]. Поэтому при проведении OSINT-исследования необходимо определять не только техническую возможность получения информации, но и ее правовой статус. Публично размещенные сведения и информация ограниченного доступа не могут рассматриваться как равнозначные категории только на том основании, что они технически обнаружены в сети Интернет.

Процессуальное значение результатов OSINT

Отдельной проблемой является использование сведений из открытых источников в уголовном процессе. Согласно уголовно-процессуальному законодательству Республики Казахстан доказательственное значение имеют фактические данные, полученные законным способом и используемые для

установления обстоятельств, подлежащих доказыванию [4]. Следовательно, обнаружение информации в открытом цифровом пространстве еще не означает автоматического приобретения ею статуса доказательства.

На первоначальном этапе результаты OSINT чаще выполняют ориентирующую функцию. Они могут способствовать установлению интересующих лиц, выявлению взаимосвязей, определению возможного местонахождения объектов либо формированию оснований для последующего проведения оперативно-розыскных и следственных мероприятий [7]. Однако при соблюдении требований к фиксации, проверке и сохранению цифровых данных отдельные материалы открытых источников могут использоваться и в материалах уголовного дела.

Практическое значение в этом отношении имеют публикации на интернет-ресурсах, содержимое веб-страниц, материалы социальных сетей, сведения о времени размещения контента, геолокационные данные и другие цифровые следы [8]. При их фиксации необходимо обеспечить возможность последующей проверки происхождения информации. Поэтому существенное значение приобретают адрес источника, дата и время получения материала, способ его обнаружения, технические условия сохранения и сопутствующие метаданные [8].

Надежность таких материалов непосредственно связана с возможностью подтвердить их неизменность после получения. Цифровая информация сравнительно легко редактируется, копируется либо удаляется. По этой причине сохранение только изображения экрана не во всех случаях позволяет установить происхождение и целостность первоначального объекта. Более обоснованным является комплексный подход, предполагающий сохранение доступного первоисточника, фиксацию его характеристик и применение технических средств контроля целостности [8].

Вместе с тем OSINT-материалы не должны оцениваться изолированно от других сведений, полученных в ходе расследования. Их достоверность может подтверждаться показаниями участников уголовного процесса, экспертными заключениями, результатами следственных действий и другими доказательствами. Такой подход соответствует принципу всесторонней оценки совокупности имеющихся фактических данных.

Методические основы работы с OSINT

Результативность использования открытых источников зависит не столько от количества обнаруженной информации, сколько от организации самого процесса поиска и ее последующей проверки. OSINT-исследование целесообразно начинать с определения конкретной задачи. Необходимо заранее установить объект поиска, требуемые категории сведений и временные пределы исследования [7]. Это позволяет ограничить массив нерелевантной информации и сделать процесс сбора воспроизводимым.

Следующий этап связан с использованием нескольких независимых информационных каналов. Общий интернет-поиск может сочетаться с анализом социальных платформ, публичных реестров, специализированных сервисов и иных доступных ресурсов [7]. При этом важно фиксировать поисковые запросы, адреса обнаруженных страниц и параметры применяемых инструментов. Подобная

фиксация дает возможность впоследствии установить последовательность получения конкретного результата.

Особое место занимает проверка достоверности обнаруженной информации. Сведения из одного источника не следует автоматически признавать достоверными. Необходимо сопоставлять их с независимыми материалами, анализировать признаки подлинности учетных записей, происхождение цифрового контента и соответствие публикаций установленным обстоятельствам [7]. При работе с интернет-ресурсами также требуется учитывать возможность подмены доменных имен, создания имитационных страниц и использования иных способов цифровой фальсификации.

Документирование процесса сбора должно обеспечивать возможность восстановления основных действий аналитика. Для значимых материалов целесообразно фиксировать URL, дату и время доступа, используемое программное обеспечение, способ обнаружения и формат сохранения объекта [8]. Если технические условия позволяют, предпочтительно сохранять исходную веб-страницу либо ее архивную копию вместе с метаданными, а не ограничиваться скриншотом.

После сохранения значимых цифровых файлов дополнительным средством контроля их неизменности может выступать вычисление криптографического хеш-значения. Его фиксация в соответствующих материалах позволяет в дальнейшем сопоставить исследуемый объект с первоначально сохраненной версией и подтвердить отсутствие изменений.

В отношении фотографий, аудио- и видеозаписей может возникнуть необходимость специальной проверки. Если достоверность такого объекта имеет существенное значение для расследования, экспертное исследование позволяет выявить признаки редактирования, монтажа или иного технического воздействия [8].

Результаты проведенного поиска должны систематизироваться таким образом, чтобы сохранялась связь между полученной информацией, ее источником и способом обнаружения. В оперативных материалах целесообразно указывать идентификаторы приложений и сведения, необходимые для последующей проверки происхождения цифрового объекта. Это способствует сохранению прослеживаемости работы с информацией на последующих этапах.

Правовая оценка должна сопровождать весь процесс OSINT-исследования. Использование открытых источников не предполагает получения доступа к закрытым ресурсам, преодоления технических ограничений или обращения к незаконно распространенным информационным массивам. В пределах OSINT должны собираться сведения, доступные без нарушения установленного законом режима доступа.

Основные риски применения OSINT

Цифровая среда содержит значительный объем недостоверной, намеренно искаженной и искусственно сформированной информации. Фальшивые учетные записи, отредактированные изображения, дезинформация и технологии создания синтетического медиаконтента способны существенно снизить надежность

результатов OSINT. Поэтому обнаруженные сведения требуют сопоставления с независимыми источниками и критической аналитической оценки.

Дополнительную сложность представляет возможность целенаправленного информационного воздействия на сотрудника, осуществляющего поиск. Интересующие правоохранительные органы лица способны сознательно размещать ложные сведения, формировать фиктивные цифровые связи или создавать информационные объекты, рассчитанные на введение аналитика в заблуждение. Снижение этого риска требует проверки принадлежности учетных записей, анализа временных характеристик публикаций и сопоставления содержания с иными независимыми данными.

Не менее существенным является обеспечение сохранности цифрового материала после его получения. Нарушение порядка хранения, отсутствие контроля изменений или невозможность установить последовательность действий с файлом способны поставить под сомнение его доказательственное значение. Минимизация подобного риска предполагает регистрацию операций с материалами, разграничение доступа и использование технических механизмов проверки целостности [9].

Отдельная группа рисков связана с конфиденциальностью оперативной и следственной деятельности. Распространение промежуточных результатов OSINT может раскрыть направления проводимой работы, интерес правоохранительных органов к конкретным объектам или иные сведения ограниченного распространения. Поэтому результаты анализа открытой информации после их включения в соответствующие служебные материалы должны обрабатываться с учетом установленного режима информационной безопасности.

Наконец, практическое применение OSINT осложняется отсутствием его специального нормативного определения. Такая ситуация может порождать неоднозначную оценку отдельных способов получения и фиксации информации [10]. Чем менее определен правовой статус применяемого метода, тем большее значение приобретает документирование обстоятельств получения сведений и подтверждение законности доступа к первоначальному источнику.

Направления совершенствования правового регулирования

Существующая модель регулирования позволяет использовать открытые информационные ресурсы при выполнении задач оперативно-розыскной деятельности, однако не формирует специального правового режима OSINT. С учетом расширения цифровой составляющей правоохранительной деятельности представляется обоснованным более четко определить место разведки по открытым источникам в системе ОРД.

Одним из возможных направлений является нормативное закрепление понятия сбора и анализа открытой информации как правомерного способа получения сведений при выполнении задач оперативно-розыскной деятельности. Такое регулирование должно одновременно устанавливать границу между работой с общедоступными источниками и действиями, связанными с получением информации ограниченного доступа. Применение OSINT не должно рассматриваться как негласный способ получения сведений, если сотрудник

использует ресурсы, доступные неопределенному кругу лиц, и не ограничивает конституционные права граждан.

Не менее важна унификация требований к цифровым материалам. Нормативное и ведомственное регулирование может предусматривать порядок фиксации источника, сохранения метаданных, контроля целостности, передачи файлов и регистрации действий с ними. Подобный подход способен повысить воспроизводимость результатов OSINT и упростить последующую оценку происхождения цифровой информации.

Практическим дополнением к законодательному регулированию могла бы стать разработка ведомственных методических рекомендаций. В них целесообразно закрепить последовательность работы с открытыми источниками, минимальные требования к верификации обнаруженных сведений, правила документирования и меры по обеспечению сохранности полученных цифровых объектов.

Заключение.

OSINT формирует дополнительные возможности для получения и анализа информации, имеющей значение для оперативно-розыскной деятельности. Его практическая ценность определяется возможностью работать с широким кругом общедоступных цифровых источников, выявлять взаимосвязи между объектами и получать сведения, способные определить дальнейшее направление оперативной или следственной работы.

Вместе с тем открытый характер источника не освобождает сотрудников правоохранительных органов от необходимости соблюдать требования законодательства. Правомерность доступа, защита персональных данных, достоверность информации, качество ее фиксации и сохранение целостности цифрового объекта непосредственно влияют на возможность последующего использования полученных материалов.

Действующее законодательство Республики Казахстан позволяет применять отдельные элементы OSINT в рамках общих норм, регулирующих оперативно-розыскную и уголовно-процессуальную деятельность. Однако отсутствие специального определения и единых методических требований сохраняет пространство для неоднозначной правовой оценки. В связи с этим дальнейшее развитие рассматриваемого направления целесообразно связать с уточнением нормативного статуса работы с открытыми источниками, стандартизацией процедур документирования цифровых материалов и разработкой ведомственных рекомендаций, учитывающих современные требования к электронным доказательствам.

Список литературы:

1. Hassan R., Hijazi M. OSINT Handbook: Guide to Open Source Intelligence. — Birmingham: University of Birmingham, 2018. — 176 p.

2. Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности» (с изм. и доп. по состоянию на 2025 г.). — ИПС «Әділет».

3. Конституция Республики Казахстан: принята на республиканском референдуме 30 августа 1995 года (с изм. и доп. по состоянию на 2024 г.). — Астана: Әділет.

4. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изм. и доп. по состоянию на 2025 г.). — ИПС «Әділет».

5. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изм. и доп. по состоянию на 2025 г.). — ИПС «Әділет».

6. Casey E. Digital Evidence and Computer Crime . — 3rd ed. — Amsterdam: Academic Press, 2011. — 838 p.

7. Europol. Open Source Intelligence in Law Enforcement . — The Hague: Europol, 2022. — 54 p.

8. United Nations Office on Drugs and Crime. Guidance on Electronic Evidence Collection . — Vienna: UNODC, 2020. — 78 p.

9. NIST. Guide to Integrating Forensic Techniques into Incident Response (SP 800-86) . — Gaithersburg: NIST, 2018. — 91 p.

10. Воронин В. Н. Оперативно-розыскная деятельность: теория и практика . — М.: Юрайт, 2021. — 312 с.

ИСКАКОВ АСЕТ КАБДЫЛХАМИТОВИЧ
Начальник кафедры служебной деятельности
уголовно-исполнительной системы
Академии управления МВД Республики Казахстан
доктор философии (PhD)

К ВОПРОСУ О СТАНОВЛЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО ПРАВА КАК САМОСТОЯТЕЛЬНОЙ ЮРИДИЧЕСКОЙ НАУКИ

Аннотация. *В статье обосновывается необходимость институционализации оперативно-розыскного права (далее – ОРП) в качестве самостоятельной фундаментально-прикладной юридической науки Республики Казахстан. Развивая ранее сформулированную авторскую концепцию о выходе ОРП на уровень самостоятельной комплексной отрасли публичного права, автор ставит научную проблему преодоления его «периферийного» или узковедомственного статуса. В работе критически анализируется процессуально-центричный подход (в частности, концепция В. И. Шарова о сведении ОРП к подотрасли уголовно-процессуального права) и приводятся аргументы в пользу его автономии. Сформулированы паспортизирующие признаки науки ОРП: разграничены предмет отрасли и предмет науки, раскрыт междисциплинарный метод, выстроена система специфических закономерностей и функций.*

Введение

В наших предыдущих исследованиях нами была обоснована необходимость выделения оперативно-розыскного права в самостоятельную комплексную отрасль публичного права, а также доказана недопустимость концепций его «неполной юридичности» и необходимость полной правовой формализации оперативной практики [1; 2].Развивая данную авторскую концепцию, мы приходим к логическому и более фундаментальному научному вопросу: почему при наличии сформированной отрасли права оперативно-розыскная наука всё еще сохраняет «периферийный» или чисто прикладной статус в системе юридических наук?

Несмотря на наличие самостоятельного предмета, специфической методологии, развитого понятийного аппарата и собственной системы закономерностей, оперативно-розыскная теория институционально продолжает восприниматься либо как междисциплинарный прикладной раздел криминалистики и уголовного процесса, либо как ведомственная спецдисциплина.

Основная часть. Становлению ОРП как науки долгое время препятствовал ряд объективных и субъективных факторов, которые в современных условиях утрачивают свое решающее значение: преодоление «ведомственного барьера» и секретности. Долгое время теория ОРД формировалась внутри закрытых ведомственных институтов, что искусственно ограничивало её академическую публичность. В XXI веке, когда ОРД всё больше опирается на открытые цифровые технологии (OSINT, Big Data, ИИ) и подпадает под жесткий контроль правозащитных институтов, секретность перестает быть препятствием для фундаментальной правовой науки.

Предметом науки ОРП являются не только нормы Закона «Об ОРД», но и закономерности правового регулирования негласного сыска, баланс между национальной безопасностью и конституционными правами, а также методология право применения.

Уголовно-процессуальная наука традиционно воспринимает ОРД лишь как «служебный» инструмент для доказывания. Однако ОРП обладает собственной превентивной, прогностической и защитной функцией (включая обеспечение национальной безопасности), выходящей далеко за рамки расследования конкретного уголовного дела.

Наука ОРП использует уникальный синтез правовых, криминолого-аналитических, специальных (оперативных) и цифровых (алгоритмических) методов; отличающийся особым сочетанием правовых, криминологических, оперативно-тактических и цифровых методов исследования.

В современной юридической доктрине вопрос о месте оперативно-розыскного права остается предметом острой теоретической дискуссии. Отдельные исследователи подходят к этой проблеме с позиций процессуального центризма. В частности, В. И. Шаров обосновывает тезис о том, что оперативно-розыскное право не обладает достаточным объемом правоотношений для статуса самостоятельной отрасли и должно рассматриваться лишь как подотрасль уголовно-процессуального права, а нормативное развитие ОРД должно идти по пути ее максимальной имплементации в УПК [3, с. 212–213].

Полагаем, что подобный подход, сводящий ОРД исключительно к «обслуживанию» уголовного судопроизводства, не учитывает современную юридическую природу негласной деятельности и существенно сужает её социальное назначение. Развивая сформулированную нами ранее авторскую концепцию [1; 2], выделим три фундаментальных контраргумента:

а) уголовный процесс строго ограничен рамками зарегистрированного уголовного правонарушения. В то же время предмет ОРП включает в себя обширный пласт превентивных, прогностических, разведывательных и контрразведывательных правоотношений (обеспечение национальной, общественной и пенитенциарной безопасности, проверка лиц при допуске к госсекретам, оперативно-аналитический поиск), где уголовное дело ещё не возбуждено и может не возникнуть вовсе. «Втискивание» этих отношений в УПК институционально невозможно.

б) Уголовно-процессуальное право ориентировано на регламентацию уголовного судопроизводства и обеспечение процессуальных гарантий участников уголовного процесса, тогда как оперативно-розыскное право регулирует более широкий комплекс отношений, связанных с выявлением угроз, предупреждением и пресечением противоправной деятельности, оперативным поиском и получением информации в условиях, когда уголовно-процессуальные отношения могут еще не возникнуть. ОРП базируется на сочетании гласных и негласных сил, средств и методов, конспирации и специфической оперативно-розыскной форме. Попытка полного процессуального «поглощения» ОРД приводит либо к разрушению конспиративного режима, либо к искусственной деформации самого уголовного

процесса (что признает и сам В. И. Шаров, отмечая, что термин «негласные следственные действия» «режет слух» [3, с. 212]).

в) Сведение правовой составляющей ОРД к УПК, а организационно-тактической – к закрытым ведомственным актам (как предлагает В. И. Шаров) фактически возвращает ОРД к до-законодательному, «ведомственному» периоду развития. Напротив, современный принцип верховенства права требует не вывода оперативной практики за рамки публичного закона, а полноценной правовой формализации (юридизации) ОРП именно как самостоятельной комплексной отрасли и науки [1].

Для окончательного обоснования ОРП в качестве самостоятельной юридической науки необходимо четко разграничить предмет отрасли права (социальные отношения) и предмет науки (теоретические закономерности, нормы, институты и практика), а также сформировать её методологический и функциональный каркас.

Предметом оперативно-розыскной науки выступает система закономерностей формирования, развития и функционирования оперативно-розыскного права, механизмов его правового регулирования и реализации, а также научно обоснованных способов обеспечения баланса эффективности оперативно-розыскной деятельности и гарантий прав и свобод личности. В него входят:

-Закономерности возникновения, развития и функционирования ОРД (включая цифровую и транснациональную преступность);

-Нормативно-правовая база и правотворческий процесс (Конституция, Закон «Об ОРД», УПК РК, подзаконные акты);

-Правоприменительная практика и оперативно-процессуальная форма (механизмы трансформации результатов ОРД в доказательства);

-Система гарантий прав и свобод личности (судебное санкционирование, прокурорский надзор, принцип соразмерности);

-Сравнительно-правовой и исторический опыт (модели investigative operations).

Наука ОРП обладает междисциплинарным комплексным методом:

Всеобщий (диалектический) метод – рассмотрение ОРП в динамике социальных и технологических трансформаций;

Формально-догматический (юридико-технический) метод – анализ дефиниций, устранение коллизий и пробелов;

Сравнительно-правовой метод – сопоставление моделей РК, стран СНГ и дальнего зарубежья;

Социолого-правовой метод – анкетирование практиков, анализ следственно-судебной практики;

Кибернетический и информационно-аналитический метод (Digital Legal Studies) – изучение правовых аспектов применения алгоритмов ИИ, Big Data и OSINT-технологий.

Закономерность причинно-следственной обусловленности: прямое влияние новых способов совершения преступлений (киберпреступность, криптотранзакции) на трансформацию правовых институтов ОРД;

Закономерность пропорциональности оперативно-розыскного вмешательства, выражающаяся в необходимости соотнесения интенсивности ограничения частных прав с характером предотвращаемой угрозы, предполагаемой эффективностью соответствующего оперативно-розыскного мероприятия и наличием процессуальных и судебных гарантий;

Закономерность «юридического опосредования» (правовой формализации): неизбежный переход эффективных фактических методов сыска в строго регламентированную законодательную форму;

Закономерность интеграции оперативных и процессуальных институтов: создание каналов передачи результатов ОРД в уголовный процесс без потери доказательственного значения.

Доктринально-регулятивная функция – Формирование концептуального понятийного аппарата, теоретических моделей законодательных актов и преодоление ведомственной разобщенности.

Методологическая функция – Обеспечение оперативных аппаратов, органов прокуратуры и суда научным инструментарием для единообразного толкования и применения норм ОРД.

Прогностическая функция – Моделирование будущих угроз национальной безопасности и разработка опережающих правовых институтов (включая правовое регулирование ИИ и цифрового профилирования).

Охранительно-гуманистическая функция – Научная разработка пределов допустимого вмешательства в частную жизнь, критериев соразмерности и механизмов защиты прав граждан от оперативного произвола.

Интегративно-прикладная функция – Синтез достижений уголовного процесса, криминалистики, криминологии, IT-права и специальной техники в единую научную систему.

Институциональные критерии становления науки ОРП является:

-наличие самостоятельного объекта и предмета исследования;

-наличие категориального аппарата;

-наличие собственной системы научных закономерностей;

-наличие методологии;

-наличие научных школ и исследовательских центров;

-наличие диссертационных исследований;

-преподавание соответствующих дисциплин;

-наличие научных публикаций;

-наличие практико-ориентированной функции;

-возможность формирования самостоятельного научного направления в системе юридических наук.

Заключение. Признание оперативно-розыскного права самостоятельной юридической наукой – это не просто терминологическая дискуссия, а необходимый шаг для модернизации системы правоохранения в XXI веке. Самостоятельность науки определяется не только наличием нормативного массива, но совокупностью самостоятельного предмета исследования, специфической системы категорий, закономерностей, методов, функций и практико-ориентированных научных задач.

Список литературы:

1. Искаков А.К., Баргаринова А.А. Теоретико-правовой анализ понятия оперативно-розыскной деятельности // Международный научный журнал «Наука-Ғылым» №1 (88), Костанай, 2026. – С. 69-76. (438с.)

2. Искаков А. К., Таженов А.Д. Место и роль оперативно-розыскной деятельности в системе правовых наук // Научный журнал «Вестник академии правоохранительных органов» №1 (39), Қосшы, 2026. – С. 172-181. (214с.).

3. Шаров В. И. Оперативно-розыскное и уголовно-процессуальное право // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2025. — № 2 (70). — С. 209–213.

КАНАШЕВ АРКАЛЫК МАНАРБЕКОВИЧ
Старший преподаватель
кафедры факультета развития профессиональных компетенций
Академии КНБ Республики Казахстан

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ В РЕСПУБЛИКЕ КАЗАХСТАН: ПРОБЛЕМЫ СОБИРАНИЯ, ПРОВЕРКИ И ИСПОЛЬЗОВАНИЯ

Цифровизация общественных отношений приводит к тому, что значительная часть информации, имеющей значение для расследования преступлений, существует в электронной форме. При совершении киберпреступлений цифровые следы могут формироваться одновременно на компьютерах и мобильных устройствах, серверах, в социальных сетях, мессенджерах, электронной почте, облачных сервисах и сетевой инфраструктуре. В результате электронная информация становится одним из важнейших источников сведений о механизме преступления и действиях его участников.

В отличие от традиционных вещественных доказательств электронные данные обладают рядом специфических характеристик: они могут быстро изменяться, удаляться, копироваться и передаваться между различными информационными системами. Кроме того, один и тот же цифровой объект может существовать одновременно в нескольких местах, а его физическое расположение не всегда совпадает с юрисдикцией государства, осуществляющего расследование. Это существенно усложняет процесс обнаружения, фиксации, сохранения и последующей оценки электронной информации.

Особую проблему представляет необходимость разграничения цифрового следа и электронного доказательства. Сам факт обнаружения цифровой информации ещё не означает её автоматического доказательственного значения. Для использования соответствующих данных в расследовании необходимо установить их происхождение, целостность, достоверность и связь с расследуемым событием. Следовательно, эффективность расследования киберпреступлений определяется не только возможностью обнаружить цифровую информацию, но и способностью обеспечить её надлежащую фиксацию и последующую проверку.

Дополнительную сложность создаёт трансграничный характер современных цифровых данных. Устройство, с которого совершено действие, может находиться в одной стране, пользователь — в другой, а сервер или облачное хранилище — в третьей юрисдикции. В таких условиях получение электронных доказательств требует не только применения национальных процессуальных механизмов, но и эффективного международного сотрудничества.

Для Республики Казахстан данная проблема приобретает особую актуальность в условиях цифровизации уголовной деятельности и развития национальной системы противодействия киберпреступности. Совершенствование работы с электронными доказательствами предполагает согласование процессуальных процедур, цифровых технологий и профессиональных компетенций специалистов. Особое значение имеет формирование единых

подходов к обнаружению, фиксации, хранению и исследованию цифровой информации.

Степень разработанности проблемы характеризуется значительным количеством исследований в области цифровой криминалистики, электронных доказательств и расследования киберпреступлений. Вместе с тем сохраняется необходимость дальнейшего изучения практических и правовых проблем работы с электронными доказательствами применительно к условиям Республики Казахстан, особенно с учётом трансграничного характера цифровой информации.

Цель исследования — определить основные проблемы собирания, проверки и использования электронных доказательств при расследовании киберпреступлений в Республике Казахстан и предложить направления совершенствования соответствующих механизмов.

Для достижения поставленной цели определены следующие задачи исследования:

1. раскрыть особенности электронных доказательств в расследовании киберпреступлений;
2. рассмотреть основные способы обнаружения, фиксации и сохранения цифровой информации;
3. определить проблемы проверки достоверности и целостности электронных доказательств;
4. рассмотреть особенности получения трансграничных цифровых данных;
5. определить направления совершенствования работы с электронными доказательствами в Республике Казахстан.

Методы исследования. В работе использованы системный, аналитический и сравнительный методы, а также анализ нормативных правовых актов и научной литературы в области уголовного процесса, цифровой криминалистики и кибербезопасности. Системный подход позволил рассмотреть электронное доказательство как элемент единого процесса расследования, а аналитический — выявить основные проблемы его получения, проверки и использования.

Электронные доказательства представляют собой цифровую информацию, которая может использоваться для установления обстоятельств совершённого преступления. В условиях киберпреступности их источниками могут выступать компьютеры, мобильные устройства, серверы, электронная почта, мессенджеры, социальные сети, облачные хранилища, сетевые журналы и другие цифровые системы.

Специфика электронных доказательств заключается в их нематериальной форме и высокой изменяемости. Цифровая информация может быть удалена, изменена, скопирована или перемещена без очевидных физических признаков такого воздействия. Поэтому при работе с ней особое значение приобретают процедуры фиксации, сохранения и подтверждения неизменности исходных данных.

В расследовании киберпреступлений необходимо различать цифровой след и доказательство. Цифровой след является источником информации, который может иметь значение для расследования, однако его доказательственное значение

возникает только после установления происхождения, достоверности, целостности и связи с обстоятельствами расследуемого события. Например, наличие определённого IP-адреса или учётной записи может свидетельствовать о совершении определённого цифрового действия, но само по себе не всегда позволяет установить конкретное лицо, осуществившее это действие.

Особое значение имеет совокупность цифровых данных. Отдельные сведения могут иметь ограниченное значение, тогда как их сопоставление позволяет восстановить последовательность событий и установить связи между пользователем, устройством, сетевым соединением и конкретным цифровым действием. Поэтому современная цифровая криминалистика ориентируется не только на обнаружение отдельных следов, но и на их комплексный анализ.

Собирание электронных доказательств представляет собой последовательный процесс обнаружения, фиксации и получения цифровой информации, имеющей значение для расследования. Особенность данного процесса заключается в необходимости сохранить не только содержание информации, но и сведения о её происхождении, времени получения и способе фиксации.

На этапе обнаружения могут исследоваться цифровые устройства, электронные документы, переписка, журналы событий, сетевые данные и иные источники цифровой информации. При этом специалисту необходимо минимизировать возможность изменения исходных данных. Любое неконтролируемое воздействие на цифровой объект потенциально способно повлиять на его последующую оценку.

Особое значение имеет фиксация цифровой информации. Она должна обеспечивать возможность установить, какие данные были получены первоначально и какие действия осуществлялись с ними в дальнейшем. В цифровой криминалистике для подтверждения неизменности данных могут использоваться специальные технические средства и криптографические механизмы, позволяющие сопоставлять исходную и исследуемую информацию.

Важным элементом является также цепочка хранения электронного доказательства (chain of custody). Она предполагает документирование последовательности действий с цифровой информацией: от момента её обнаружения до последующего исследования и представления в рамках расследования. Необходимо фиксировать, кто получил доступ к данным, когда это произошло, каким способом информация была сохранена и передавалась ли она другим специалистам.

Проблема сохранения особенно актуальна для цифровых данных, которые могут находиться на удалённых серверах или в облачных системах. В таких случаях необходимо учитывать не только техническую возможность получения информации, но и условия её хранения, возможность изменения или удаления и соответствующие правовые основания доступа.

Одной из наиболее сложных задач при использовании электронных доказательств является установление их достоверности и связи с расследуемым событием. Цифровая информация может быть изменена, скопирована или представлена в искажённом виде, поэтому сам факт её обнаружения ещё не гарантирует достоверность полученного сведения.

Особое значение имеет установление источника цифровой информации. Например, наличие определённой учётной записи, IP-адреса или устройства может свидетельствовать о совершении цифрового действия, однако не всегда позволяет однозначно установить лицо, которое его совершило. Для этого необходимо сопоставлять несколько источников информации и учитывать контекст совершённого действия.

Проверка электронного доказательства должна включать оценку его целостности, происхождения и способа получения. Если невозможно установить, каким образом информация была обнаружена, сохранена и исследована, возникают сомнения в возможности объективной оценки её содержания. Поэтому техническая процедура работы с цифровыми данными непосредственно связана с их последующей доказательственной оценкой.

Важную роль в данном процессе играет специалист, обладающий необходимыми техническими и криминалистическими компетенциями. Его задача заключается не только в извлечении информации, но и в обеспечении возможности её последующей проверки. При этом технический вывод специалиста и юридическая оценка доказательства не должны смешиваться: установление технического факта не означает автоматически установления юридически значимого обстоятельства.

Современные киберпреступления часто имеют трансграничный характер: лицо, совершившее преступление, может находиться в одной стране, используемое устройство — в другой, а сервер или облачное хранилище с необходимыми данными — в третьей. В результате получение электронных доказательств выходит за пределы национальной юрисдикции и требует взаимодействия между государствами.

Особую проблему представляет получение данных у иностранных поставщиков цифровых и телекоммуникационных услуг. Следственные органы могут нуждаться в информации об учётных записях, соединениях, электронных сообщениях, платежах или иных цифровых действиях, однако доступ к таким сведениям регулируется законодательством государства, на территории которого находится соответствующий поставщик или инфраструктура.

В этих условиях важную роль играет международное сотрудничество в сфере противодействия киберпреступности. Обмен информацией, правовая помощь, взаимодействие правоохранительных органов и использование согласованных процедур получения цифровых данных позволяют повысить эффективность расследований, которые невозможно провести исключительно национальными средствами.

Для Казахстана данное направление приобретает особое значение в связи с необходимостью участия в международных механизмах противодействия киберпреступности. Трансграничный характер цифровых доказательств требует совершенствования процедур их оперативного получения, проверки происхождения и обеспечения допустимости последующего использования в национальном уголовном процессе.

Совершенствование работы с электронными доказательствами в Республике Казахстан должно быть направлено на обеспечение единого и последовательного

подхода к их обнаружению, фиксации, сохранению, исследованию и оценке. В условиях быстрого развития цифровых технологий существующих общих процессуальных механизмов может быть недостаточно для решения всех технических вопросов, возникающих при расследовании киберпреступлений.

Одним из приоритетных направлений является стандартизация процедур работы с цифровой информацией. Необходимо обеспечить единые требования к фиксации исходных данных, созданию цифровых копий, документированию действий специалистов и обеспечению цепочки хранения электронного доказательства. Это позволит снизить вероятность утраты или изменения информации и повысить воспроизводимость результатов исследования.

Важное значение имеет развитие профессиональных компетенций специалистов. Работа с электронными доказательствами требует сочетания знаний уголовного процесса, криминалистики, информационной безопасности и цифровых технологий. Поэтому подготовка кадров должна включать не только технические навыки извлечения данных, но и понимание процессуальных требований к их фиксации и представлению.

Необходимым направлением является также совершенствование механизмов **международного получения электронных доказательств**. Поскольку значительная часть цифровых данных может храниться за пределами Казахстана, эффективность расследований будет зависеть от скорости взаимодействия с иностранными правоохранительными органами и поставщиками цифровых услуг.

Перспективным представляется внедрение специализированных цифровых платформ, обеспечивающих документирование жизненного цикла электронного доказательства. Такая система могла бы фиксировать этапы получения, хранения, передачи и исследования информации, формируя единый цифровой журнал действий с доказательственным объектом.

В обобщённом виде предлагаемый подход можно представить следующим образом:

ОБНАРУЖЕНИЕ → ФИКСАЦИЯ → ИЗЪЯТИЕ → СОХРАНЕНИЕ → ИССЛЕДОВАНИЕ → ПРОВЕРКА → ОЦЕНКА → ПРОЦЕССУАЛЬНОЕ ИСПОЛЬЗОВАНИЕ.

Проведённый анализ показывает, что электронные доказательства приобретают ключевое значение при расследовании современных киберпреступлений. Цифровые следы, формируемые на различных устройствах, серверах, сетевых ресурсах и онлайн-платформах, позволяют устанавливать обстоятельства совершённого деяния и восстанавливать последовательность событий.

Вместе с тем специфика цифровой информации создаёт дополнительные требования к её собиранию и использованию. Электронные данные могут изменяться, удаляться и копироваться, поэтому их доказательственная ценность непосредственно связана с возможностью подтвердить происхождение, целостность и способ получения соответствующей информации.

Особое значение имеет разграничение цифрового следа и электронного доказательства. Обнаружение цифровой информации само по себе не означает её доказательственного значения. Необходимы её надлежащая фиксация, сохранение,

техническое исследование и последующая оценка в совокупности с другими материалами расследования.

Дополнительную сложность создаёт трансграничный характер цифровых данных. Распределение устройств, пользователей и серверов между различными юрисдикциями делает международное сотрудничество важнейшим условием эффективного расследования киберпреступлений.

Для Республики Казахстан перспективными направлениями являются стандартизация процедур работы с электронными доказательствами, совершенствование механизмов их международного получения, развитие профессиональных компетенций специалистов и внедрение технологических решений для документирования жизненного цикла цифровых данных.

Список литературы:

1. Уголовно-процессуальный кодекс Республики Казахстан: Кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. – URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 18.08.2026).

2. Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК. – URL: https://adilet.zan.kz/rus/docs/K2600000255 (дата обращения: 18.08.2026). Новый Кодекс содержит нормы об электронных документах, цифровых документах и требованиях к достоверности и неизменности цифровой информации.

3. О некоторых вопросах оценки доказательств по уголовным делам: нормативное постановление Верховного Суда Республики Казахстан от 20 апреля 2006 года № 4 (с изменениями и дополнениями). – URL: https://adilet.zan.kz/rus/docs/P06000004S (дата обращения: 18.08.2026). Документ прямо предусматривает возможность использования компьютерной информации и устанавливает необходимость оценки её достоверности, относимости и допустимости.

4. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. – Geneva: International Organization for Standardization, 2012.

5. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. – Gaithersburg: National Institute of Standards and Technology, 2006. – 121 p. – (NIST Special Publication 800-86). – DOI: 10.6028/NIST.SP.800-86.

6. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. – 6th ed. – Boston: Cengage Learning, 2019. – 752 p.

7. Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest, 23 November 2001. – CETS No. 185. – URL: https://www.coe.int/en/web/cybercrime/convention-on-cybercrime (дата обращения: 18.08.2026). Конвенция содержит процессуальные инструменты для получения и сохранения электронных доказательств и механизмы международного сотрудничества.

8. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). – Strasbourg: Council of Europe, 2022. – 49 p.

9. Otebaliyeva K. E., Sharipova A. B. Classification of electronic evidence in the criminal process // *Eurasian Science Review: An International Peer-reviewed Multidisciplinary Journal*. – 2026. – DOI: 10.63034/esr-695. Работа непосредственно посвящена правовой природе и классификации электронных доказательств в уголовном процессе.

10. Цифровая криминалистика: особенности современной методики расследования // *Вестник Актюбинского регионального университета имени К. Жубанова*. – 2026. – URL: https://vestnik.arsu.kz/index.php/hab/article/view/912 (дата обращения: 18.08.2026). В работе рассматриваются современные методы цифровой криминалистики, электронные доказательства и практические вопросы их исследования.

КАРЛ АРДАК МАРАТОВИЧ
Начальник кафедры кибербезопасности и информационных технологий Костанайской академии МВД Республики Казахстан имени Шракбека Кабылбаева
кандидат юридических наук

ШАХМАТОВ АЛЕКСАНДР ВЛАДИМИРОВИЧ
Профессор кафедры оперативно-разыскной деятельности в органах внутренних дел Санкт-Петербургского университета МВД России
доктор юридических наук, профессор,
заслуженный сотрудник ОВД Российской Федерации

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: РОЛЬ И МЕСТО КИБЕРБЕЗОПАСНОСТИ

В современных условиях цифровой трансформации оперативно-розыскная деятельность приобретает особую актуальность. Развитие информационных технологий, расширение цифрового пространства и появление новых форм киберпреступности обусловливают необходимость совершенствования форм, методов и средств оперативно-розыскной деятельности. В этих условиях особое значение приобретает кибербезопасность как важная составляющая противодействия преступности в цифровой среде.

Актуальность выбранной темы обусловлена тем, что оперативно-розыскная деятельность непосредственно связана с обеспечением общественной безопасности и борьбой с преступностью, а в условиях цифровизации именно киберсреда становится основной площадкой противоправной активности.

В ранее проведённых исследованиях по проблемам оперативно-розыскной деятельности авторами высказывалась позиция о целесообразности сохранения действующего законодательства с внесением в него точечных изменений и дополнений. [1, с. 74]. Однако на тот период проблематика киберпреступности и цифровых угроз не носила столь системного характера, как сегодня. В современных условиях подобный подход уже не отражает объективную реальность и требует пересмотра.

Сегодня можно уверенно говорить о необходимости разработки нового закона об оперативно-розыскной деятельности, отвечающего требованиям цифровой эпохи.

Схожие дискуссии ведутся и в других государствах постсоветского пространства в контексте реформирования законодательства и трансформации института оперативно-розыскной деятельности [2, с. 346–432; 3, с. 250]. Это свидетельствует об общности современных вызовов и актуализирует необходимость дальнейшего научного осмысления вопросов развития ОРД в условиях цифровизации.

Переходя к основному содержанию, отметим, что в Республике Казахстан создана рабочая группа по разработке проекта нового закона об оперативно-розыскной деятельности. Данная инициатива обусловлена необходимостью адаптации законодательства к современным условиям цифровизации и трансформации преступной среды. Представляется, что вопросы дальнейшего совершенствования законодательства об оперативно-розыскной деятельности актуальны и для Российской Федерации, в том числе в части его адаптации к новым технологическим реалиям и особенностям противодействия преступности в цифровой среде.

В практической деятельности оперативных подразделений сохраняется ряд правовых и организационных проблем. В частности, в законодательстве Республики Казахстан после принятия нового Уголовно-процессуального кодекса из числа задач оперативно-розыскной деятельности было исключено «раскрытие преступлений», что актуализировало вопрос о роли и пределах участия субъектов ОРД в доведении оперативных разработок до логического завершения.

Кроме того, субъекты оперативно-розыскной деятельности лишены права инициировать и самостоятельно проводить негласные следственные действия, что сформировало правовой разрыв между оперативно-розыскными мероприятиями и негласными следственными действиями.

Особого внимания заслуживает профилактическая функция оперативно-розыскной деятельности. В современных условиях предупреждение преступлений приобретает особое значение, однако профилактический потенциал ОРД остается реализованным не в полной мере. Особенно актуальным данный вопрос становится в цифровой среде, где оперативное выявление угроз и рисков способно способствовать предупреждению преступлений еще на стадии их подготовки.

Одним из ключевых направлений развития оперативно-розыскной деятельности становится внедрение технологий искусственного интеллекта. В Республике Казахстан правовые основы их применения получили дальнейшее развитие с принятием Закона «Об искусственном интеллекте» [4]. В Российской Федерации также проводится последовательная работа по формированию нормативных основ разработки и применения технологий искусственного интеллекта [5]. В этой связи особую актуальность приобретает исследование возможностей использования ИИ в оперативно-розыскной деятельности и противодействии киберпреступности.

Уже сегодня рассматриваются возможности применения нейросетевых и аналитических технологий при проведении оперативно-розыскных мероприятий, включая:

- анализ больших массивов данных;
- мониторинг интернет-пространства;
- выявление цифровых следов преступной деятельности.

В этой связи требует актуализации сам перечень оперативно-розыскных мероприятий. Современная практика объективно диктует необходимость включения таких форм, как:

- киберразведка и кибермониторинг;
- использование алгоритмов машинного обучения;

- применение беспилотных летательных аппаратов;
- расширение традиционных ОРМ с учётом цифровых и технических средств.

Международная практика показывает эффективность отказа от института понятых в пользу обязательной видеофиксации, а также применение единой санкции на комплекс специальных оперативно-розыскных мероприятий [6, с. 308].

Одним из направлений совершенствования законодательства представляется расширение возможностей субъектов оперативно-розыскной деятельности по технической реализации мероприятий, связанных с использованием сетей связи. В данном контексте заслуживает внимания опыт Российской Федерации, где соответствующие мероприятия проводятся с использованием оперативно-технических сил и средств как органов федеральной службы безопасности, так и органов внутренних дел. Представляется целесообразным рассмотреть возможность применения аналогичного подхода и в Республике Казахстан при сохранении надлежащего контроля и надзора за законностью проведения таких мероприятий.

Анализ зарубежного опыта более чем 20 государств показывает, что нормы оперативно-розыскной деятельности в них органично интегрированы в уголовный процесс, а современные технические средства доступны всем субъектам. Широко применяются:

- видеофиксация вместо понятых;
- технологии искусственного интеллекта и Big Data;
- расширенные профилактические механизмы.

Подводя итог, следует отметить, что дальнейшее развитие законодательства об оперативно-розыскной деятельности должно учитывать современные процессы цифровизации, новые формы преступности, возможности искусственного интеллекта и возрастающую роль кибербезопасности. Современная модель ОРД должна сочетать традиционные формы оперативной работы с цифровыми технологиями, превентивной направленностью и надежными правовыми гарантиями защиты прав личности.

Представленные положения носят дискуссионный характер и требуют дальнейшего научного осмысления, экспертного обсуждения и сравнительно-правового анализа.

Полагаем, что дальнейший научный диалог и обмен опытом между Российской Федерацией и Республикой Казахстан будут способствовать совершенствованию правовых и организационных основ оперативно-розыскной деятельности в условиях цифровой трансформации.

Список литературы:

1. Карл А.М. Законодательное регулирование оперативно-розыскных мероприятий в Российской Федерации и Республике Казахстан» (сравнительно-правовое исследование): монография / А.М. Карл, А.В. Шахматов. – Алматы: ADAL KITAP, 2026. – 211 с.
2. Сурков К.В. Оперативно-розыскное законодательство России: пути совершенствования и развития: дис. … д-ра юрид. наук: 12.00.09 / Сурков Константин Викторович. – Москва, 1997. – 432 с.
3. Галахов С.С. Проблемы правовой основы оперативно-розыскной деятельности и пути совершенствования законотворческой деятельности в этой сфере (к юбилею принятия Федерального

закона «Об оперативно-розыскной деятельности») // Теория и практика общественного развития. – 2025. – № 11. – С. 247–253.

4. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII (с изменениями от 25.08.2026 г.) [Электронный ресурс] // Сайт «PRG». – Режим доступа: https://prg.kz/document/?doc_id=34207749 (дата обращения: 1.09.2026).

5. О поддержке развития технологий искусственного интеллекта в Российской Федерации: Федеральный закон от 26.07.2026 N 243-ФЗ [Электронный ресурс] // СПС КонсультантПлюс. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_529215/ (дата обращения: 1.09.2026).

6. Валитов Р.А. К вопросу о целесообразности существования и развития института понятых в уголовном процессе / Р.А. Валитов // Молодой ученый. – 2023. – № 18 (465). – С. 307-309.

КАУАЗОВ САНАК КАЗКЕНОВИЧ
Старший преподаватель
кафедры факультета развития профессиональных компетенций
Академии КНБ Республики Казахстан

РЕКОНСТРУКЦИЯ СОБЫТИЙ ПО ЦИФРОВЫМ СЛЕДАМ В СОВРЕМЕННОЙ КРИМИНАЛИСТИКЕ: ВОЗМОЖНОСТИ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

Цифровизация общественных отношений сопровождается изменением характера преступной деятельности и расширением количества цифровых следов, которые могут возникать в процессе подготовки, совершения и сокрытия преступления. Компьютеры, мобильные устройства, серверы, сетевые журналы, электронная почта, мессенджеры и облачные сервисы сохраняют различные цифровые артефакты, позволяющие реконструировать действия пользователей и последовательность происходивших событий. Современная цифровая криминалистика рассматривает реконструкцию событий как самостоятельное направление, основанное на анализе совокупности цифровых артефактов.

Одной из основных проблем является **разрозненность цифровой информации**. Следы одного события могут одновременно находиться на нескольких устройствах и в различных информационных системах. При этом отдельный цифровой артефакт не всегда позволяет установить полный механизм произошедшего. Его криминалистическое значение раскрывается при сопоставлении с другими следами, их временными характеристиками и контекстом расследуемого события.

В связи с этим особое значение приобретает восстановление **хронологии цифровых событий**. Построение временной последовательности позволяет определить, какие действия были совершены, в какой момент они произошли и каким образом отдельные события связаны между собой. Однако такая реконструкция осложняется неоднородностью цифровых данных, большим их объёмом, различиями в форматах временных меток, ошибками системного времени и возможным намеренным изменением цифровых следов.

Реконструкция событий имеет существенное значение для расследования киберпреступлений, поскольку позволяет перейти от анализа отдельных цифровых следов к восстановлению **целостной последовательности действий**. Это способствует установлению механизма преступления, выявлению взаимосвязей между участниками и устройствами, а также проверке различных версий произошедшего. Вместе с тем результаты такой реконструкции требуют критической оценки, поскольку временные метки и цифровые артефакты могут содержать технические искажения или подвергаться намеренному воздействию.

Для Республики Казахстан развитие данного направления приобретает практическое значение в условиях роста преступлений с цифровым компонентом и повышения требований к профессиональной подготовке правоохранительных органов. В 2026 году Академия правоохранительных органов при Генеральной

прокуратуре Республики Казахстан проводила специализированную подготовку по цифровой криминалистике, включая вопросы источников цифровых доказательств, их обнаружения, фиксации и изъятия. Это показывает актуальность формирования профессиональных компетенций, необходимых для анализа цифровых следов и их использования в расследовании.

Степень разработанности проблемы характеризуется развитием исследований в области цифровой криминалистики и timeline-based event reconstruction. Вместе с тем современные исследования отмечают фрагментарность существующих подходов и необходимость формирования более системной методологии реконструкции цифровых событий.

Цель исследования — определить криминалистические возможности и основные проблемы реконструкции событий на основе цифровых следов при расследовании преступлений в Республике Казахстан.

Для достижения поставленной цели определены следующие задачи исследования:

1. раскрыть значение цифровых следов для криминалистической реконструкции событий;
2. рассмотреть основные источники цифровых артефактов;
3. определить особенности построения хронологии цифровых событий;
4. выявить основные проблемы интерпретации временных и иных цифровых меток;
5. определить перспективы применения реконструкции цифровых событий в практике расследования преступлений в Казахстане.

Методы исследования. В работе использованы системный, аналитический и сравнительный методы, а также анализ научной литературы в области цифровой криминалистики и реконструкции цифровых событий. Системный подход позволил рассмотреть цифровые следы как взаимосвязанную совокупность криминалистической информации, а аналитический — определить возможности и ограничения их использования для восстановления хронологии расследуемого события.

Цифровой след представляет собой информацию, которая сохраняется в результате действий пользователя, работы программного обеспечения или функционирования информационной системы. К таким следам могут относиться файлы, записи системного реестра, журналы событий, история браузера, данные приложений, сетевые соединения и другие цифровые артефакты. Их совокупный анализ позволяет устанавливать отдельные обстоятельства произошедшего и восстанавливать последовательность действий. Современные исследования рассматривают реконструкцию событий как процесс вывода о прошлой активности на основе анализа цифровых артефактов.

Особенностью цифрового следа является то, что он обычно отражает не само событие, а его цифровое проявление. Например, запись о создании или изменении файла свидетельствует о соответствующем изменении состояния системы, но для установления конкретного действия пользователя требуется сопоставление этой информации с другими источниками.

Поэтому отдельный цифровой артефакт редко позволяет получить полную картину произошедшего. Существенное криминалистическое значение возникает при объединении данных из нескольких источников: компьютера, мобильного устройства, сетевых журналов, облачного сервиса или приложения. Такой подход позволяет перейти от анализа отдельных следов к построению единой временной последовательности.

Особую роль в этом процессе играют временные характеристики цифровых данных. Временные метки позволяют расположить отдельные записи в определённом порядке, однако их нельзя воспринимать как абсолютно точное отражение реального времени события. Системные часы могут быть неправильно настроены, подвергаться естественному дрейфу, техническим сбоям или намеренному изменению.

В связи с этим при реконструкции необходимо учитывать источник временной информации и сопоставлять различные временные показатели. Современный подход предполагает использование так называемых временных якорей (time anchors) — цифровых артефактов, позволяющих сопоставить системное время с более надёжным внешним источником времени.

Реконструкция хронологии цифровых событий представляет собой процесс установления последовательности действий на основе совокупности цифровых артефактов. В цифровой криминалистике такой подход позволяет перейти от анализа отдельных следов к восстановлению целостной картины произошедшего. Современные исследования рассматривают timeline-based event reconstruction как самостоятельное направление цифровой криминалистики, при этом отмечается необходимость более системного подхода к его методологии. Ọ

Основой реконструкции является объединение информации, полученной из различных источников. Например, данные о входе в систему, создании или изменении файла, подключении устройства и сетевом соединении сами по себе характеризуют отдельные действия. Их расположение в единой временной последовательности позволяет установить взаимосвязь между событиями и предположить возможный механизм действий пользователя.

Особое значение имеет сопоставление цифровых следов из разных источников. Если несколько независимых систем фиксируют связанные события, их совместный анализ повышает обоснованность реконструкции. При этом специалист должен учитывать возможные противоречия между источниками и не рассматривать автоматически совпадение временных меток как доказательство причинно-следственной связи.

Важным этапом является определение временного интервала расследуемого события и последующее размещение цифровых артефактов внутри этого интервала. Такой подход позволяет отделить непосредственно связанные с расследуемым событием данные от фоновой активности системы. В современной литературе подчёркивается, что реконструкция должна учитывать не только объём доступных данных, но и различные факторы, способные повлиять на интерпретацию цифровых событий. Ọ

При этом хронология не должна восприниматься как абсолютно объективная последовательность. Она представляет собой криминалистическую реконструкцию,

основанную на доступных цифровых артефактах и определённых аналитических выводах. Поэтому каждое существенное событие должно по возможности подтверждаться несколькими независимыми источниками, а неопределённость и возможные альтернативные объяснения должны фиксироваться отдельно.

Одним из ключевых элементов реконструкции цифровых событий являются временные метки, позволяющие определить последовательность действий пользователя и функционирования системы. Однако их интерпретация не всегда является однозначной. Системное время устройства может отличаться от реального времени события вследствие неправильной настройки, часового пояса, технического сбоя или дрейфа системных часов.

Дополнительную сложность создаёт наличие нескольких устройств и информационных систем, каждая из которых может использовать собственные настройки времени. Поэтому одинаковое событие, зафиксированное в разных источниках, может иметь различные временные значения. При построении единой хронологии необходимо учитывать эти различия и приводить данные к сопоставимому временному контексту.

Особую опасность представляет намеренное изменение временных параметров. Лицо, стремясь скрыть следы своей деятельности, потенциально может воздействовать на системное время или иным способом затруднить установление реальной последовательности действий. Поэтому временная метка должна рассматриваться не как абсолютный факт, а как цифровой артефакт, требующий проверки.

Одним из подходов к решению данной проблемы является использование временных якорей (time anchors) — данных, позволяющих сопоставить системное время с более надёжным внешним источником. Такой подход помогает определить возможное смещение времени и повысить обоснованность последующей реконструкции.

Не менее важным является сопоставление временных данных из различных источников. Например, запись о входе в систему, сетевое соединение и создание файла могут иметь разные временные отметки. Их совместный анализ позволяет установить наиболее вероятную последовательность событий, одновременно выявляя возможные противоречия.

Следовательно, время в цифровой криминалистике должно рассматриваться не просто как технический параметр, а как объект криминалистического анализа. Надёжная реконструкция требует проверки временных меток, определения возможных искажений и сопоставления нескольких независимых источников. Именно такой подход позволяет снизить риск ошибочной интерпретации цифровых событий и повысить достоверность реконструированной хронологии. Современные исследования подчёркивают, что проблемы временных меток являются одной из самостоятельных групп трудностей timeline-based event reconstruction.

Реконструкция цифровых событий позволяет перейти от анализа отдельных артефактов к восстановлению предполагаемой последовательности действий, связанных с расследуемым преступлением. Её основная задача заключается в установлении взаимосвязи между отдельными цифровыми событиями и определении наиболее обоснованной последовательности их возникновения.

Современные исследования рассматривают такую реконструкцию как отдельное направление цифровой криминалистики и подчёркивают необходимость системного анализа цифровых артефактов.

Практически реконструкция может включать сопоставление различных типов данных: входа пользователя в систему, создания и изменения файлов, запуска программ, сетевых соединений, подключения внешних устройств, удаления информации и других действий. Например, последовательность вход в систему → создание файла → его изменение → подключение внешнего носителя → удаление файла → сетевое соединение может позволить сформировать криминалистическую гипотезу о развитии события.

Особое значение имеет выявление связей между событиями. Само по себе совпадение нескольких временных отметок ещё не доказывает наличие причинно-следственной связи. Поэтому специалисту необходимо учитывать источник каждого цифрового следа, особенности его формирования, достоверность временных данных и возможные альтернативные объяснения.

Реконструкция может использоваться для проверки следственных версий. Если установленная последовательность цифровых событий соответствует одной версии и противоречит другой, результаты анализа могут служить основанием для её дальнейшей проверки. При этом реконструированная последовательность должна рассматриваться именно как результат криминалистического анализа, а не как автоматически установленная истина. Исследователи отмечают, что современные подходы к timeline-based reconstruction сталкиваются с целым комплексом неопределённостей и ограничений, которые необходимо учитывать при интерпретации результатов.

Применение реконструкции цифровых событий в практике расследования связано с рядом ограничений. Одной из основных проблем является значительный объём и разнородность цифровой информации. Следы могут поступать из различных устройств, операционных систем, приложений и сетевых сервисов, что требует их сопоставления и приведения к единому аналитическому контексту. Современные исследования отмечают, что проблемы реконструкции не сводятся только к объёму данных и включают также особенности цифровых артефактов, инструментов анализа и решений самого эксперта.

Другой проблемой является неполнота цифрового следа. Часть информации может быть удалена пользователем, автоматически перезаписана системой или оказаться недоступной вследствие особенностей работы конкретного сервиса. Поэтому отсутствие определённого цифрового артефакта не всегда означает отсутствие соответствующего действия.

Существенное значение имеет и квалификация специалиста. Реконструкция предполагает не просто автоматическое построение временной шкалы, а интерпретацию взаимосвязей между различными цифровыми событиями. Ошибка на этапе отбора или интерпретации данных способна привести к формированию неверной последовательности. Поэтому результаты реконструкции должны быть проверяемыми и по возможности воспроизводимыми.

Для Казахстана перспективным направлением является формирование единых методических подходов к реконструкции цифровых событий в рамках

цифровой криминалистики. Целесообразно стандартизировать порядок работы с временными метками, правила сопоставления цифровых артефактов и требования к документированию полученных результатов. Такой подход позволит уменьшить зависимость итоговых выводов от индивидуальной методики конкретного специалиста.

Перспективным является также использование специализированных программных средств, способных автоматически объединять цифровые артефакты в единую временную шкалу. Однако автоматизация должна рассматриваться как инструмент поддержки специалиста, а не как замена криминалистической интерпретации. Современная концепция Timeline-based Event Reconstruction Model (TER-Model) как раз направлена на систематизацию различных этапов и проблем реконструкции цифровых событий.

Для практики расследования в Казахстане предлагаемая модель может быть представлена следующим образом:

Сбор цифровых артефактов → проверка источников → синхронизация временных данных → построение хронологии → сопоставление событий → выявление связей → реконструкция механизма → проверка выводов.

Проведённый анализ показывает, что реконструкция событий по цифровым следам становится важным направлением современной цифровой криминалистики. Совокупность цифровых артефактов позволяет не только фиксировать отдельные действия пользователей и информационных систем, но и восстанавливать их предполагаемую последовательность. При этом современная литература подчёркивает, что методология timeline-based event reconstruction пока остаётся фрагментированной, что обусловливает необходимость систематизации терминологии, процедур и критериев оценки результатов.

Особое значение имеет комплексное сопоставление цифровых следов, полученных из различных источников. Отдельный артефакт не всегда позволяет установить содержание и обстоятельства события, тогда как их объединение во временную последовательность способствует выявлению взаимосвязей между действиями, устройствами и пользователями. Вместе с тем реконструированная хронология должна рассматриваться как результат криминалистического анализа, а не как автоматически установленная последовательность фактов.

Одной из наиболее существенных проблем остаётся достоверность временных характеристик цифровых данных. Различия в настройках системного времени, часовых поясах, технические ошибки и возможное намеренное изменение временных параметров способны повлиять на итоговую реконструкцию. Поэтому временные метки требуют проверки и сопоставления с другими независимыми цифровыми источниками.

Для Республики Казахстан развитие данного направления представляется перспективным в контексте совершенствования национальной цифровой криминалистики. Целесообразным является формирование единых методических подходов к анализу цифровых артефактов, работе с временными данными и документированию результатов реконструкции.

Список литературы:

1. Breitinger F., Studiawan H., Hargreaves C. **SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges** // *Forensic Science International: Digital Investigation*. – 2025. – Vol. 53. – Art. 301932. – DOI: 10.1016/j.fsidi.2025.301932.

2. Vanini C., Hargreaves C. J., van Beek H., Breitinger F. **Was the clock correct? Exploring timestamp interpretation through time anchors for digital forensic event reconstruction** // *Forensic Science International: Digital Investigation*. – 2024. – Vol. 49. – Art. 301759. – DOI: 10.1016/j.fsidi.2024.301759.

3. **A common framework to situate digital and physical traces in time** // *Forensic Science International*. – 2024. – Vol. 360. – Art. 112020. – DOI: 10.1016/j.forsciint.2024.112020.

4. Studiawan H., Breitinger F., Scanlon M. **Towards a standardized methodology and dataset for evaluating LLM-based digital forensic timeline analysis** // *Forensic Science International: Digital Investigation*. – 2025. – Vol. 54. – Art. 301982. – DOI: 10.1016/j.fsidi.2025.301982.

5. Vanini C., Gruber J., Hargreaves C., Benenson Z., Freiling F., Breitinger F. **Understanding strategies and challenges of timestamp tampering for improved digital forensic event reconstruction** // *Proceedings of the Digital Forensics Doctoral Symposium (DFDS '25)*. – New York: ACM, 2025. – DOI: 10.1145/3712716.3712727.

6. Casey E. **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**. – 3rd ed. – London: Academic Press, 2011. – 800 p.

7. Carrier B. **File System Forensic Analysis**. – Boston: Addison-Wesley, 2005. – 600 p.

8. Kent K., Chevalier S., Grance T., Dang H. **Guide to Integrating Forensic Techniques into Incident Response**. – Gaithersburg: National Institute of Standards and Technology, 2006. – 121 p. – (NIST Special Publication 800-86). – DOI: 10.6028/NIST.SP.800-86.

9. Garfinkel S. **Digital forensics research: The next 10 years** // *Digital Investigation*. – 2010. – Vol. 7. – P. S64–S73. – DOI: 10.1016/j.diin.2010.05.009.

10. Nelson B., Phillips A., Steuart C. **Guide to Computer Forensics and Investigations**. – 6th ed. – Boston: Cengage Learning, 2019.

КАУНОВ АЛЕКСАНДР ВЛАДИМИРОВИЧ
начальник кафедры оперативно-разыскной деятельности органов внутренних дел Всероссийского института повышения квалификации сотрудников МВД России (ВИПК МВД России), кандидат юридических наук подполковник полиции

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ В ПРОТИВОДЕЙСТВИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В сложившихся условиях постоянное совершенствование оперативно-розыскной деятельности (далее – ОРД), направленной на борьбу с организованной преступностью, становится необходимостью. Насколько успешно выполняется эта задача, во многом зависит от того, как быстро правоохранительные органы успевают приспосабливаться к меняющимся формам и методам, которыми пользуются организованные группы (далее – ОГ), а также преступные сообщества (далее – ПС). Особое внимание следует уделять модернизации тактики и стратегии оперативно-розыскных мероприятий (далее – ОРМ), а также внедрению новейших технологий в деятельность оперативных подразделений органов внутренних дел (далее – ОВД).

Ключевым вектором развития в ближайшие годы станет создание межведомственной цифровой экосистемы. Сегодня разрозненность баз данных различных силовых структур, в том числе МВД России, ФСБ России, Росгвардии и Федеральной налоговой службы, способствует замедлению оперативной работы. Переход к концепции единого доступа к аналитическим данным позволит правоохранительным органам видеть полную картину преступной деятельности: от момента регистрации юридического лица до совершения транзакции и перемещения конкретного фигуранта по территории страны.

Интеграция ведомственных систем в единый облачный контур с использованием защищенных каналов связи позволит сократить время принятия решений с дней до минут. В условиях, когда ОГ и ПС действуют транснационально и молниеносно, такая скорость реакции становится критическим фактором успеха.

Существенное значение имеет расширение применения информационно-аналитических систем ОВД. Использование автоматизированных баз данных, технологий распознавания лиц и голоса, а также современных методов обработки больших массивов информации на базе искусственного интеллекта позволяет выявлять скрытые связи между преступниками, заблаговременно прогнозировать их вероятные действия и точнее планировать проведение ОРМ. Вместе с этим требуется надежно защищать конфиденциальность подобных сведений, а также выстраивать механизмы их оперативного обмена как между различными оперативными подразделениями ОВД, так и между правоохранительными органами России в целом.

Системы распознавания лиц, интегрированные в городскую инфраструктуру, стали мощнейшим инструментом. В крупных мегаполисах России, таких как Москва, сеть камер с функцией биометрической идентификации позволяет находить лиц, находящихся в федеральном розыске, в режиме реального времени. Это не просто «цифровой глаз», а инструмент, который делает скрытное передвижение преступников по стране практически невозможным.

Будущее борьбы с организованной преступностью лежит в плоскости внедрения систем предиктивного моделирования. Речь идет о создании цифровых двойников криминогенных зон, где алгоритмы искусственного интеллекта, анализируя исторические данные, социально-экономические показатели и текущую оперативную обстановку, смогут прогнозировать всплески преступной активности. Это позволит правоохранительным органам переходить от модели «тушения пожаров» к модели их предотвращения, перераспределяя патрули и оперативные группы в те точки, где риск совершения преступления наиболее высок.

Внедрение столь мощных инструментов контроля неизбежно ставит вопрос о границах допустимого вмешательства в частную жизнь. Для того, чтобы «цифровой щит» не превратился в инструмент избыточного давления, необходимо выстраивание прозрачной системы общественного и парламентского контроля. Технологии должны быть подотчетны закону, а алгоритмы принятия решений – проходить регулярный аудит на предмет отсутствия предвзятости. Доверие граждан к государственным цифровым системам – это фундамент, без которого невозможно эффективное взаимодействие общества и правоохранительных органов в эпоху тотальной цифровизации.

Отсутствие в системе правоохранительных органов Российской Федерации подразделения, специализирующегося на противодействии организованной преступности, а также должного правового регулирования правоотношений, связанных с борьбой с организованной преступностью, приводит к тому, что в правоприменительной деятельности оперативные сотрудники ОВД, занимающиеся выявлением, предупреждением, пресечением и раскрытием преступлений, совершаемых представителями ОГ и ПС, сталкиваются с проблемой наличия большого количества функций и обязанностей у оперативных сотрудников ОВД, в должностные обязанности которых входит борьба с организованной преступностью.

Нельзя недооценивать роль правовой базы, которая должна соответствовать современным вызовам. Законодательство, регулирующее ОРД, должно быть гибким и своевременно обновляться, чтобы охватывать все новые формы и методы противоправной деятельности.

В настоящее время особенно остро стоит вопрос о правовом регулировании отношений, связанных с противодействием организованной преступности. Если будет принят Федеральный закон «О борьбе с организованной преступностью», ОРМ в контексте противодействия организованной преступности станут более действенными, так как их ориентируют на фиксацию преступной деятельности лидеров и наиболее активных участников ОГ и ПС. Помимо этого, подобный закон позволит более точно обозначить понятийный аппарат и детально установить правовые и организационные основы мероприятий, которые будут использовать

сотрудники оперативных подразделений ОВД для противодействия организованным формам преступности.

Данной точки зрения придерживается С.Д. Белоцерковский, который отмечает, что на законодательном уровне назрела необходимость принятия межотраслевого федерального закона «О борьбе с организованной преступностью», включающего применение как общих положений, как и специфических мер по данному направлению оперативно-служебной деятельности [1, с. 266; 2, с. 51; 3, с. 95].

Справляться с актуальными угрозами, которые исходят от представителей уголовно-криминальной среды, удается не только благодаря увеличению числа технических средств. Не менее важно изменить сами подходы к ОРД, на которые опираются сотрудники оперативных подразделений ОВД. Отдельного внимания требует поиск и внедрение новых способов фиксации и подтверждения доказательств, прежде всего в цифровом пространстве. Для этого необходимо установить порядок сбора цифровых улик, обучить специалистов работе с криминалистическим программным обеспечением, а также создать надежные каналы для передачи и хранения цифровых данных. Насколько успешно ведется борьба с организованной преступностью, в том числе с киберпреступностью, зависит от того, способны ли оперативные сотрудники ОВД действовать на опережение, заранее выявлять новые направления атак и быстро отвечать на возникающие уязвимости.

Ключевым фактором в этой борьбе призвано стать развитие превентивных мер, направленных на выявление и пресечение преступных намерений представителей ОГ и ПС на ранних стадиях. Это предполагает более глубокое изучение психологии представителей уголовно-криминальной среды, выявление их внутренней структуры, мотивов и потенциальных угроз. Применение методов прогнозирования и моделирования, основанных на анализе криминальной статистики и поведенческих паттернов, может стать мощным инструментом в руках оперативных сотрудников.

Следует заключить, что сложность документирования организованных форм преступности заключается в том, что преступные группировки часто действуют скрытно, имеют четкую иерархию, но при этом не всегда оставляют явные следы своей структуры. Доказывание сговора, распределения ролей и устойчивости группы требует кропотливой работы следственных и оперативных подразделений ОВД, использования специальных знаний и применения сложных тактических приемов.

Мы стоим на пороге эры, где противодействие организованной преступности будет осуществляться не только в физическом пространстве, но и в виртуальной среде, где границы между ними окончательно сотрутся. Развитие квантовых вычислений и технологий распределенных реестров (блокчейн) потребует от государства еще более глубокой технологической трансформации.

Россия обладает мощным интеллектуальным потенциалом для того, чтобы стать лидером в создании высокотехнологичных систем безопасности. Инвестиции в отечественное программное обеспечение, развитие киберполигонов для обучения сотрудников и поддержка инновационных разработок в сфере криминалистики –

это те инвестиции, которые окупаются безопасностью каждого гражданина. В конечном счете, победа над организованной преступностью в XXI веке будет одержана не только силой закона, но и силой интеллекта, воплощенного в коде и алгоритмах.

В конечном счете, успех оперативных подразделений ОВД в деле противодействия организованной преступности зависит от комплексного подхода, включающего технологическую модернизацию, а также совершенствование законодательства. Только такой многогранный подход позволит правоохранительным органам оставаться на шаг впереди организованных форм преступности и обеспечивать безопасность граждан.

Использование современных технических возможностей – это уже не опция, а необходимость. Сегодня борьба с организованной преступностью в России – это интеллектуальное противостояние. Побеждает тот, у кого быстрее алгоритмы, точнее аналитика и эффективнее взаимодействие между ведомствами. Будущее за созданием единой цифровой экосистемы, где технологии будут не просто помогать сотрудникам правоохранительных органов, а станут его главным союзником в обеспечении безопасности общества.

Список литературы:

1. Белоцерковский С. Д. Комплексный закон в системе правового регулирования борьбы с организованной преступностью // Пробелы в российском законодательстве. – 2017. – № 6. – С. 266–268.
2. Белоцерковский С. Д. Организованная преступность в системе угроз национальной безопасности Российской Федерации // Вестник Российской правовой академии. – 2017. – № 4. – С. 48–51.
3. Белоцерковский С. Д. Система правового регулирования борьбы с организованной преступностью: её структура и содержание // Пробелы в российском законодательстве. – 2017. – № 5. – С. 95–97.

КЕНЖЕЕВ СУЛТАН САКЕНОВИЧ
докторант 2 курса Академии управления
МВД Республики Казахстан
магистр права

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ КАК ИНСТРУМЕНТЫ СОВЕРШЕНСТВОВАНИЯ ИССЛЕДОВАНИЯ ВЕЩЕСТВЕННЫХ ДОКАЗАТЕЛЬСТВ В ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

Стремительное развитие технологий искусственного интеллекта позволяющая обработать большие объёмы информации, анализа структурно сложных данных сделало его наиболее эффективным инструментом в цифровой криминалистике. Интеграция технологий искусственного интеллекта в цифровую криминалистику формирует новые возможности для автоматизации и повышения эффективности криминалистического исследования. Применение алгоритмов интеллектуального анализа данных позволяет обрабатывать значительные объемы цифровой информации, осуществлять ее структурирование и квалификацию, выявлять релевантные сведения и устанавливать возможности между отдельными информационными объектами. Это создает предпосылки для совершенствования методов обнаружения и исследования вещественных доказательств, содержащих цифровые следы. Современные исследования в области фиксации, хранения и использования электронной (цифровой) информации в качестве доказательств все больше ориентированы на применение технологий искусственного интеллекта при обработке, анализе и криминалистическом исследовании данных, содержащихся на электронных носителях и иных объектах, имеющих доказательственное значение.

Указанные процессы предпосылки для совершенствования методов обнаружения, фиксации и исследования вещественных доказательств, содержащих цифровую информацию и цифровые следы. Особенность таких объектов заключается в сочетании материальной формы носителя и информационного содержания, исследование которого требует применения специальных знаний, технических средств и соответствующих криминалистических методов. А.О.Бессонова, исследуя электронные носители как разновидность вещественных доказательств, обращает внимание на их специфическое свойства, особенности формирования и необходимости соблюдения специальных правил собирания и исследования содержащейся в них информации [1].

Современные исследования вопросов фиксации, хранения и использования электронной (цифровой) информации в доказывании все больше затрагивают возможности применения новых методов ее обработки. Особый научный интерес представляет использование искусственного интеллекта для анализа значительных объемов разнородных данных, поскольку алгоритмическая обработка позволяет не только ускорить поиск информации, но и выявлять признаки и взаимосвязи, обнаружение которых посредством традиционного последовательного

исследования требует значительных временных ресурсов. Т.К.Рябина, Д.О.Чистилина и Я.П.Ряплова рассматривая цифровую трансформацию уголовно-процессуального доказывания, выделяют внедрение систем искусственного интеллекта в доказательственную деятельность в качестве одного из направлений происходящих преобразований [2]. Вместе с тем возможности искусственного интеллекта применительно к исследованию вещественных доказательств не следует сводить исключительно к автоматизации поиска цифровой информации. Более существенное значение приобретает интеллектуальный анализ данных, позволяющий осуществлять классификацию исследуемых объектов, распознавание отдельных признаков, сопоставлению значительных информационных массивов, выявление повторяющихся элементов и установление скрытых связей между различными источниками криминалистических значимых сведений. Международные исследование цифровой криминалистики свидетельствуют о развитии специализированных технологических решений, использующих искусственный интеллект и расширенную аналитику данных для правоохранительной деятельности. В частности, в зарубежной литературе рассматриваются проекты AIDA *(Искусственный интеллект и аналитика данных для правоохранительных органов)* и ALIGNER *(Дорожная карта внедрения исскуственного интелекта в деятельность полиции и правоохранительных органах)* ориентированные на использование возможностей искусственного интеллекта при обработке информации правоохранительными органами [3].

При этом внедрение алгоритмических методов в процесс исследования доказательственной информации формирует новые требования к достоверности и проверяемости полученных результатов. Использование искусственного интеллекта предполагает появление дополнительного технологического элемента между исходным объектом и результатом его исследования-алгоритма, посредством которого осуществляется обработка данных. Следовательно, значение приобретает не только эффективность применяемого программного средства, но и возможность установить происхождение исходных данных, последовательность произведенных с ними операций, обеспечить сохранение их первоначального состояния и во производимость полученного результата.

Практика Республики Казахстан свидетельствует о постепенном переходе от использывания отдельных цифровых средств к внедрению интелектуальных систем поддержки расследования. В деятельности органов уголовного преследования получают развитие технологии алгоритмического анализа больших массивов данных, автоматизированной индификации и классификации информации, распознования и преоброзования речи, сопоставления речи, сопоставления сведений, построения информационных связей и прогнозной аналитики. А.Б.Айтуарова и Ж.Ә.Жарылкасынов отмечают применение в казахстанской практике систем видеонаблюдения с элементами распознавания лиц, алгоритмического анализа больших данных, автоматизированной индикации лиц и событий, а также программных средств прогнозирования и квалификации информации[4]. Вопрос прослеживаемости приобретает особое значение применительно к вещественным доказательствам. А.А.Толыбаев, А.Ж.Исаев, Ш.Р.Жумагулов, Э.Ашимов и Д.У.Байтукаева анализируя развитие электронного

уголовного судопроизводства Казахстана, отмечают сохраняющиеся проблемы цифровой фиксации вещественных доказательств в электронное уголовное дело. В качестве одного из направлений совершенствования ими предлагается внедрение модуля учета вещественных доказательств с использыванием QR-маркировки, а так же дальнейшая интеграция информационных систем посредством Data Hub [5]. Представляется, что дальнейшее развитие данного направления связано с объединением цифрового учета вещественных доказательств и интеллектуального анализа содержащейся в них информации. При таком подходе искусственный интеллект может использоваться не для замены следователя или эксперта, а для предварительного анализа, систематизации и сопоставления значительных объемов криминалистических значимых данных. Исходный объект, сведения о его обнаружении и изъятии, результаты цифровой фиксации и последующей алгоритмической обработки должны при этом образовать прослеживаемую последовательность, позволяющую проверить происхождение и неизменность исследуемой информации.

Одним из наиболее показательных примеров практического внедрения искусственного интелекта является реализуемый Министерством внутренних дел Республики Казахстан проекты «Помощник следователя AI». Функциональные возможности системы включают автоматизированную обработку материалов Единого реестра досудебных расследований (ЕРДР), формирование проекта плана расследования, построение схем взаимосвязей между участниками уголовного процесса, обработку и сопоставление показаний, выявление содержащихся в них противоречий, подготовку процессуальных документов, а так же анализ и прогнозирование данных. Дополнительным направлением является применение технологии распознавания речи *(SPEECH-TO-TEXT)* для преобразования аудио и видеоматериалов следственных действий в текстовую форму [6]. Наряду с этим в деятельность МВД Республики Казахстан внедряется информационная система «е-Айғақзат», предназначенная для цифровизации процессов учета и контроля вещественных доказательств [7]. «е-Айғақзат» предназначенная для цифровизации процессов учета и контроля вещественных доказательств. Ее применение представляет особый интерес для цифровой криминалистики, поскольку формирование цифрового учета движения вещественных доказательств создает организационно-техническую основу для последующей интеграции сведений об объектах с инструментами интеллектуального анализа данных.

Одним из самостоятельных направлений внедрения искусственного интеллекта в правоохранительную деятельность Республики Казахстан становится интеллектуальная обработка значительных массивов правовой, статистической и криминологических значимой информации. В данном аспекте представляет интерес деятельность Центра прогнозирования преступных угроз Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Аналитическая деятельность Центра осуществляется с использованием больших данных, межведомственного информационного обмена и инструментов искусственного интеллекта. В числе внедренных решений называются системы мониторинга медиа пространства и интернет-мошенничеств, анализ обращений, поступающих посредством информационной системы «е-Өтініш», а также модели

прогнозирования уличной и повторной преступности [8]. Применение подобных технологий свидетельствует о постепенном изменении самого подхода к информационно-аналитическому обеспечению правоохранительной деятельности. Если традиционный анализ преимущественно предполагает последовательное изучение уже систематизированных сведений по заранее установленным критериям, то технологии искусственного интеллекта позволяют осуществлять обработку значительно более крупных массивов данных, выявлять повторяющиеся признаки и зависимости, осуществлять их группировку и формировать аналитические результаты для последующей профессиональной оценки. При этом принципиально важно разграничивать автоматизированную обработку информации и принятие процессуального решения: выявленная алгоритмом статистическая зависимость, аномалия либо информационная связь сама по себе не свидетельствует о доказанности обстоятельства уголовного правонарушения и требует последующей проверки компетентным субъектом.

Развитие практики применения искусственного интеллекта для обработки значительных массивов данных получило отражение в разработке Генеральной прокуратурой Республики Казахстан пилотного инструмента «ИИ-аналитик Больших Данных». Данная нейросетевая система способна обработать годовой массив криминальной статистики приблизительно за 15 минут и сформировать интерактивные аналитические панели, отражающие, в частности, демографические показатели и виды правонарушений [9].

Научная значимость указанных разработок заключается не столько в увеличении скорости обработки информации, сколько в изменении методики работы с большими массивами криминалистических значимых данных. Искусственный интеллект позволяет перейти от последовательного изучения отдельных информационных объектов к их комплексному сопоставлению. В результате объектом аналитической обработки становится не единичный документ или отдельная запись, а совокупность взаимосвязанных сведений, в которой алгоритм способен выделять совпадающие признаки, устойчивые зависимости, нетипичные отклонения и связи, требующие последующей проверки.

Для исследования вещественных доказательств такой подход имеет перспективное значение. В ходе расследования сведения об одном материальном объекте могут быть распределены между различными источниками: протоколом его обнаружения и изъятия, фотографиями и видеозаписями, заключением эксперта, информацией электронного носителя, результатами осмотра, данными криминалистических учетов и иными материалами уголовного дела. При значительном количестве объектов установление взаимосвязей между соответствующими сведениями традиционным способом становится трудоемким. Поэтому интеллектуальный анализ потенциально может использоваться для сопоставления информации о вещественных доказательствах, поиска совпадающих признаков, установления информационных связей между объектами и выделения данных, требующих углубленного экспертного или следственного исследования. Вместе с тем использование искусственного интеллекта применительно к доказательственной информации требует разграничения поисково-аналитического и доказательственного значения полученного результата. Алгоритмически

установленная связь между объектами может служить основанием для выдвижения версии, определения направления дальнейшего исследования или поиска дополнительной информации, однако сама по себе не должна рассматриваться как установленный доказательственный факт. В этом проявляется вспомогательная природа искусственного интеллекта. Алгоритм способен существенно расширить аналитические возможности следователя и эксперта, но окончательная интерпретация выявленных закономерностей должна осуществляться человеком с учетом происхождения исходных данных, способа их получения и совокупности других материалов уголовного дела.

Заключение

Применение искусственного интеллекта и интеллектуального анализа данных постепенно становится одним из перспективных направлений развития цифровой криминалистики. Реализуемые в Республике Казахстан проекты «Помощник следователя AI», «е-Айғақзат» и инструменты анализа больших данных демонстрируют возможности автоматизированной обработки значительных объемов информации, выявления взаимосвязей между данными и информационно-аналитической поддержки расследования.

Применительно к исследованию вещественных доказательств потенциал искусственного интеллекта заключается в возможности комплексного сопоставления сведений, содержащихся в протоколах следственных действий, экспертных заключениях, фото и видеоматериалах, электронных носителях, криминалистических учетах и иных информационных источниках. Вместе с тем результат алгоритмической обработки не должен самостоятельно приобретать доказательственное значение. Выявленные системой признаки, зависимости и взаимосвязи требуют обязательной проверки следователем, специалистом или экспертом и последующей процессуальной оценки.

В этой связи предлагается использовать модель «алгоритмическое выявление – профессиональная проверка – процессуальная оценка». Одновременно представляется целесообразным разработать единые методические требования к применению искусственного интеллекта при обработке криминалистически значимой информации, предусматривающие сохранение исходных данных, фиксацию произведенных системой операций, возможность воспроизведения результатов и обязательный контроль со стороны уполномоченного субъекта.

Таким образом, искусственный интеллект следует рассматривать не как замену следователя или эксперта, а как вспомогательный интеллектуально-аналитический инструмент, расширяющий возможности обнаружения и исследования криминалистически значимой информации. Такой подход позволит использовать преимущества современных технологий при сохранении требований достоверности, проверяемости и процессуальной допустимости результатов исследования вещественных доказательств.

Список литературы:

1. Бессонова А.О. Электронный носитель информации как разновидность вещественного доказательства в уголовном процессе // Вестник Удмуртского университета. Серия Экономика и право. -2024. -Т. 34. -Вып. 5. – С. 892-897. DOI: 10.35634/2412-9593-2024-34-5-892-897.

2. Рябинина Т.К., Чистилина Д.О., Ряполова Я.П. Цифровая трансформация уголовно-процессуального доказывания: преимущества и риски // Вестник Томского государственного университета. – 2025. -№ 516. – С. 223–236. DOI: 10.17223/15617793/516/25.

3. Halefom H. Abraha. Law enforcement access to electronic evidence across borders: mappingpolicy approaches and emerging reform initiatives. International Journal of Law and Informa-tion Technology, 29(2):118–153, 2021.

4. Жарылкасынов К.Ә., Айтуарова А.Б. Проблемы допустимости и оценки доказательств, полученных с использованием искусственного интеллекта, в уголовном судопроизводстве.// // Eurasian Scientific Journal of Law. – 2026. – № 2(102).

5. Tolybayeva A., Isayeva A., Zhumagulova Sh., Ashimova E., Baitukayeva D. Problems of Electronic Criminal Procedure in Kazakhstan and Comparative Analysis of Foreign Digital Investigation Models // Вестник КазНУ. Серия юридическая. -2025. -№ 4 (116). -С. 125 и далее. -DOI: 10.26577/JAPJ2025116411.

6. В МВД внедряют искусственный интеллект в работу следователей [Электронный ресурс] // Официальный интернет-ресурс МВД РК. –//https://www.gov.kz/memleket/entities/qriim/press/news/details/1034235?lang=ru&utm_source=chatgpt.com// (дата обращения: 20.08.2026).

7. Цифровые проекты МВД Республики Казахстан: «Цифровой помощник следователя», «е-Айғақзат», «Видео НД» [Электронный ресурс] // Министерство внутренних дел РК: официальный интернет-ресурс. –

//https://www.gov.kz/memleket/entities/qriim/press/news/details/1199158?lang=ru&utm_source=chatgpt.com// (дата обращения: 20.08.2026).

8. Цифровые решения и искусственный интеллект: Генеральная прокуратура развивает современные инструменты обеспечения правопорядка [Электронный ресурс] // ГП РК: официальный интернет-ресурс. -//https://www.gov.kz/memleket/entities/prokuror/press/news/details/1229493?lang=ru&utm_source=chatgpt.com// (дата обращения: 20.08.2026).

9. Казахстан переходит в лигу стран, где правоохранительная деятельность опирается на науку о данных и машинный интеллект: прокуроры стали ИИ-разработчиками и представили свои продукты мировому эксперту Кай-Фу Ли [Электронный ресурс] // ГП РК: официальный интернет-ресурс. https://www.gov.kz/memleket/entities/prokuror/press/news/details/1268887?lang=ru&utm_source=chatgpt.com (дата обращения20.08.2026).

КОНВИСАРЬ АННА АНДРЕЕВНА
Заместитель начальника кафедры
общеюридических дисциплин Костанайской академии
МВД Республики Казахстан имени Ш.Кабылбаева
полковник полиции

ЭТИКО-ОРГАНИЗАЦИОННЫЕ РИСКИ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНУЮ ДЕЯТЕЛЬНОСТЬ: БАЛАНС МЕЖДУ ЭФФЕКТИВНОСТЬЮ И ЗАЩИТОЙ ПРАВ ЧЕЛОВЕКА

Стремительное развитие технологий искусственного интеллекта (далее – ИИ) закономерно затрагивает сферу обеспечения правопорядка. Системы интеллектуального видеонаблюдения, автоматизированного распознавания лиц и государственных регистрационных номеров, обработки больших массивов оперативно-разыскной информации и поддержки принятия решений всё активнее внедряются в практическую деятельность органов внутренних дел Республики Казахстан.

Значимым шагом в институционализации государственной политики в данной сфере стало принятие Закона Республики Казахстан от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте», вступившего в силу по истечении шестидесяти календарных дней после его официального опубликования (по данным ряда источников – 18 января 2026 года) и закрепившего риск-ориентированный подход к регулированию систем ИИ в зависимости от степени их воздействия на безопасность пользователей, общества и государства [1]. Закон прямо провозглашает человека, его жизнь, права и свободы высшей ценностью в процессах создания и эксплуатации систем искусственного интеллекта и закрепляет требование сохранения автономии и свободы воли человека при их эксплуатации [1]. Примечательно, что статья 13 закона прямо выводит специальные государственные органы из-под ряда общих обязанностей по предоставлению данных оператору национальной платформы ИИ, что оставляет открытым вопрос о специфике применения риск-ориентированного регулирования именно в правоохранительной и специальной сферах [1].

Вместе с тем расширение сферы применения интеллектуальных систем в правоохранительной деятельности порождает комплекс рисков, которые условно можно разделить на организационные (качество данных, кадровое обеспечение, распределение ответственности внутри ведомства) и этико-правовые (алгоритмическая дискриминация, вторжение в частную жизнь, снижение уровня процессуальных гарантий). Специфика правоохранительной сферы состоит в том, что ошибка алгоритма здесь способна повлечь не экономические потери, а необоснованное преследование и ограничение свободы личности.

В практике правоохранительных органов Республики Казахстан можно выделить несколько устойчивых направлений применения технологий ИИ. Во-первых, это интеллектуальное видеонаблюдение и распознавание государственных регистрационных номеров транспортных средств – наиболее развитое на

сегодняшний день направление, представленное системой «Сергек». Современные камеры системы оснащены инфракрасной подсветкой и работают в высоком разрешении, что позволяет распознавать номерной знак, а также фиксировать использование ремня безопасности и иные детали даже в условиях недостаточной освещённости [2].

Во-вторых, развивается направление биометрической идентификации личности: по состоянию на 2021 год, согласно заявлению сооснователя проекта «Сергек» К. Ахметова, функция распознавания лиц на камерах ещё не была внедрена, однако отмечалось техническое наличие такой возможности и её потенциальное использование в дальнейшем – после соответствующих законодательных решений и общественного обсуждения. Он также уточнил, что камеры «Сергек» устанавливаются не только на дорогах, но и в общественных местах [3]. Впоследствии полномочия камер были расширены: по сообщениям профильных изданий, Министерство внутренних дел Республики Казахстан прорабатывает вопрос фиксации цифровыми системами не только нарушений правил дорожного движения, но и иных административных правонарушений, что также обусловило появление в экспертной среде сомнений в достаточной точности идентификации граждан.

В-третьих, развивается централизованная инфраструктура видеомониторинга, аккумулирующая метаданные – атрибуты объектов и лиц, попадающих в объектив, – с привязкой к временной метке [4], что приближает казахстанскую практику к моделям «безопасного города», реализуемым в странах Центральной Азии с использованием оборудования зарубежных производителей [5]. В-четвёртых, развивается направление судебно-экспертной деятельности: в Казахстане ведётся разработка обновлённой версии системы судебной экспертизы «Е-сараптама 2.0» с применением ИИ, призванной повысить точность и скорость исследований в дополнение к уже действующей интеграции с Единым реестром досудебных расследований [6]. Данное направление также требует самостоятельного юридического осмысления и унифицированного понятийного аппарата.

Общей чертой перечисленных направлений выступает то, что решения, прежде принимавшиеся исключительно человеком – сотрудником полиции, дознавателем, экспертом, – частично делегируются алгоритму либо принимаются с опорой на его рекомендации. Именно эта особенность порождает основной массив этико-организационных рисков, рассматриваемых далее.

К числу организационных рисков относится, прежде всего, риск недостаточной технической точности алгоритмов. Применительно к расширению функционала системы «Сергек» на дополнительные составы административных правонарушений эксперт – главный редактор журнала «За рулём Казахстан» А. Алексеев – указывает на сомнения в точности распознавания лиц и корректности идентификации граждан. [7]. По оценке юриста Б. Онгарова, нейросеть системы способна ошибочно принять посторонний предмет (например, пачку салфеток или футляр от очков) за телефон в руке водителя из-за плохого освещения, бликов на лобовом стекле или неудачного угла съёмки [8]. Подобные погрешности,

некритичные при фиксации нарушений ПДД, приобретают иное значение при их использовании для идентификации личности и привлечения к ответственности.

Вторым риском выступает дефицит специализированной нормативно-технической базы: до вступления в силу Закона «Об искусственном интеллекте» эксплуатация систем видеоаналитики регулировалась преимущественно общими нормами о персональных данных, не учитывающими специфику алгоритмических систем. Закон вводит понятие систем ИИ высокой степени риска, однако правоприменительная практика по этим нормам применительно к правоохранительной сфере только формируется [1].

Третий риск связан с непрозрачностью условий взаимодействия с поставщиками технологий, значительная часть которых имеет иностранное происхождение: если в соседних странах региона (Таджикистан, Узбекистан) отмечается практика грантового и кредитного финансирования проектов «умного» видеонаблюдения зарубежными государствами, то в Казахстане преобладает закупка технологий «под ключ» у зарубежных производителей – в частности, компании Hikvision, наиболее популярного поставщика технологии распознавания лиц в стране. В обоих случаях это ставит вопрос о независимом контроле государства над используемыми алгоритмами [5]. Наконец, следует отметить ненадёжность защиты персональных данных в рамках централизованной платформы, аккумулирующей метаданные о значительной части населения страны: по оценке экспертов, подобные системы сопряжены с риском утечек и продажи собранных сведений третьим лицам [4].

Центральное место среди этических рисков занимает алгоритмическая предвзятость (algorithmic bias). Поскольку модель ИИ отражает статистические закономерности обучающей выборки, недостаточная представленность отдельных социальных или демографических групп в исходных данных приводит к систематически более высокой частоте ошибочной идентификации и ложных срабатываний в отношении таких групп [9]. Применительно к правоохранительной сфере это означает риск непропорционального внимания правоохранительных органов к отдельным категориям граждан, что вступает в противоречие с закреплённым в статье 16 Конституции Республики Казахстан принципом равенства всех перед законом и судом [10], а равно с прямым запретом дискриминации при создании и эксплуатации систем ИИ, установленным Законом «Об искусственном интеллекте» [1].

Второй риск – снижение прозрачности и объяснимости принимаемых решений («проблема чёрного ящика»), особенно значимая при автоматической фиксации правонарушений системами видеонаблюдения: гражданину зачастую затруднительно установить, на основании каких данных и с какой достоверностью алгоритм квалифицировал его действия как противоправные. Это ограничивает реализацию права на обжалование, поскольку ни заявитель, ни правоприменитель не всегда способны реконструировать логику вывода системы.

Третий риск – эрозия персональной ответственности должностных лиц («размывание ответственности»), при которой сотрудник, формально принимающий решение, фактически руководствуется рекомендацией алгоритма. Закон «Об искусственном интеллекте» стремится минимизировать данный риск,

закрепляя требование сохранения автономии и свободы воли человека при эксплуатации систем ИИ и право пользователя отказаться от взаимодействия с ней, когда это прямо не предписано законом [1].

Четвёртый риск связан с массовым сбором биометрических и иных персональных данных при развёртывании общенациональной системы видеомониторинга [4], охватывающей не только дороги, но и общественные места крупных городов [3]. Это создаёт предпосылки для несоразмерного ограничения права на неприкосновенность частной жизни, гарантированного статьёй 21 Конституции Республики Казахстан, на фоне ограниченного общественного контроля за условиями внедрения таких технологий в регионе [10].

Как уже было обозначено, ключевым событием в правовом регулировании ИИ в Республике Казахстан стало принятие Закона «Об искусственном интеллекте». Закон закрепляет риск-ориентированный подход к классификации систем ИИ, возлагает на их собственников обязанность принимать меры по минимизации ущерба правам физических лиц вплоть до приостановки эксплуатации системы, а также провозглашает человека, его права и свободы высшей ценностью в процессах создания и эксплуатации ИИ [1]. Правительством утверждён перечень подзаконных актов, необходимых для реализации закона [11].

Закон устанавливает и меры юридической ответственности за неправомерное использование ИИ: административная ответственность – за причинение вреда высокой степени риска, повлёкшего дискриминацию, нарушение прав человека или иной вред, если деяние не содержит признаков уголовно наказуемого деяния [12]; по данным того же источника, уголовная ответственность по пп.3. ч.2. ст. 274 Уголовного кодекса Республики Казахстан наступает за создание и распространение посредством ИИ заведомо ложной информации (в частности, дипфейков), причинившее существенный вред правам граждан [12].Специальных же норм, детально регламентирующих применение систем видеоаналитики и биометрической идентификации именно в правоохранительной деятельности, действующее регулирование пока не содержит.

Наиболее последовательный подход к правовому регулированию применения ИИ правоохранительными органами демонстрирует законодательство Европейского союза. Регламент (ЕС) 2024/1689 (AI Act) относит большинство систем ИИ, используемых в правоохранительной деятельности, к категории систем высокого риска (Приложение III, п. 6), предъявляя к ним повышенные требования в части качества данных (ст. 10), документирования (ст. 11), человеческого надзора (ст. 14) и права на обжалование (ст. 86), а системы удалённой биометрической идентификации в реальном времени в общедоступных местах допускает лишь в исключительных, прямо предусмотренных законом случаях (ст. 5(1)(h)) [13]. Данный подход отражает попытку нормативно закрепить именно тот баланс между эффективностью и защитой прав человека, о необходимости которого говорится в настоящей статье: технология не запрещается полностью, но её применение обусловливается системой процедурных гарантий, соразмерных степени риска.

Сопоставление казахстанского и зарубежного опыта показывает, что принятый Закон «Об искусственном интеллекте» заложил современную рамочную конструкцию риск-ориентированного регулирования, сопоставимую по логике с

европейской моделью. Вместе с тем детализация применительно к правоохранительной деятельности – статус результатов автоматической фиксации правонарушений, основания биометрической идентификации, процедура обжалования решений – нуждается в дальнейшей проработке на уровне подзаконных актов, часть которых уже включена в утверждённый Правительством перечень мер по реализации закона [11].

На основе проведённого анализа можно сформулировать ряд направлений, обеспечивающих сочетание эффективности применения ИИ и защиты прав человека в правоохранительной деятельности Республики Казахстан. Во-первых, необходима разработка специального подзаконного акта (правил, положения), детально регламентирующего порядок применения систем видеоаналитики и биометрической идентификации органами внутренних дел, включая перечень допустимых целей их использования, требования к точности алгоритмов и порядок независимой сертификации в соответствии с риск-ориентированным подходом, заложенным Законом «Об искусственном интеллекте».

Во-вторых, требуется закрепление принципа обязательного человеческого контроля («human-in-the-loop»): результат работы алгоритма, включая автоматическую фиксацию правонарушений системой «Сергек», должен рассматриваться как ориентирующая информация, подлежащая проверке уполномоченным должностным лицом. В-третьих, необходимо установление обязательных процедур независимого технического аудита алгоритмов на предмет точности идентификации и дискриминационного эффекта.

В-четвёртых, целесообразно повышение прозрачности условий взаимодействия с иностранными поставщиками технологий, включая раскрытие основных характеристик используемых алгоритмов и порядка обработки собираемых данных. В-пятых, необходимо обеспечить реальные процессуальные гарантии для граждан, включая право на мотивированное разъяснение основания принятого решения и право на его обжалование – данное право соотносится с закреплённым Законом правом пользователя запрашивать информацию о данных, на основании которых системой ИИ принято решение.

Наконец, важным организационным условием выступает системная подготовка кадров органов внутренних дел Республики Казахстан к работе с интеллектуальными системами, включающая техническую составляющую и формирование этической культуры критического отношения к автоматизированным рекомендациям.

Проведённый анализ показывает, что внедрение искусственного интеллекта в правоохранительную деятельность Республики Казахстан – прежде всего в форме интеллектуального видеонаблюдения и биометрической идентификации на базе системы «Сергек» – сопровождается взаимосвязанным комплексом организационных и этико-правовых рисков: от недостаточной технической точности алгоритмов и фрагментарности специального регулирования до алгоритмической предвзятости, непрозрачности принимаемых решений и эрозии персональной ответственности должностных лиц. Специфика правоохранительной сферы состоит в том, что цена подобных рисков напрямую затрагивает фундаментальные права и свободы личности, гарантированные Конституцией

Республики Казахстан, – право на равенство, неприкосновенность частной жизни, судебную защиту и человеческое достоинство.

Принятие Закона Республики Казахстан «Об искусственном интеллекте» стало значимым шагом в институционализации риск-ориентированного подхода к регулированию систем ИИ и закреплении приоритета прав и свобод человека при их эксплуатации. Вместе с тем достижение разумного баланса между эффективностью применения интеллектуальных технологий и защитой прав человека в правоохранительной деятельности возможно лишь при условии дальнейшей детализации закона применительно к специфике полицейской практики: закрепления обязательного человеческого контроля, регулярного независимого аудита алгоритмов, прозрачности условий взаимодействия с поставщиками технологий и реальных процессуальных гарантий для граждан. Опыт Европейского союза, закрепившего дифференцированный подход к регулированию ИИ-систем в зависимости от степени риска, представляется значимым ориентиром для развития соответствующих подзаконных актов Республики Казахстан в данной сфере.

Список литературы:

1. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII (с изм. и доп. от 25.08.2026 г.) // https://prg.kz/document/?doc_id=34207749 (дата обращения: 27.08.2026).

2. Как и что видят новые камеры «Сергек»? Абсолютно всё? [Электронный ресурс] // Kolesa.kz. URL: https://kolesa.kz/content/news/kak-i-chto-vidyat-novye-kamery-sergek-absolyutno-vsyo/ (дата обращения: 27.08.2026).

3. Будут ли распознавать лица камеры «Сергек», ответил сооснователь проекта [Электронный ресурс] // Казинформ. URL: https://www.inform.kz/ru/budut-li-raspoznavat-lica-kamery-sergek-otvetil-soosnovatel-proekta_a3749729 (дата обращения: 27.08.2026).

4. Большой брат: как будет работать национальная система видеомониторинга в Казахстане [Электронный ресурс] // Forbes Kazakhstan. URL: https://forbes.kz/articles/bolshoy_brat_po-kazahski_1582187734 (дата обращения: 27.08.2026).

5. Спрятаться не получится. Как в Центральной Азии строят антиутопию с распознаванием лиц [Электронный ресурс] // Медиазона Центральная Азия. URL: https://mediazona.ca/article/2024/02/28/face-recognition (дата обращения: 27.08.2026).

6. Минюст Казахстана внедрит ИИ в систему судебных экспертиз [Электронный ресурс] // KAZINFORM. // https://www.inform.kz/ru/minyust-kazahstana-vnedrit-ii-v-sistemu-sudebnih-ekspertiz-ae581e (дата обращения: 27.08.2026).

7. Штрафы по-новому: сомнения о распознавании лиц через «Сергек» выразил эксперт [Электронный ресурс] // Orda.kz. URL: https://orda.kz/shtrafy-po-novomu-somnenija-o-raspoznavanii-lic-cherez-sergek-vyrazil-jekspert-412193/ (дата обращения: 27.08.2026).

8. Штраф за телефон с камеры «Сергек»: как доказать свою правоту и обжаловать наказание [Электронный ресурс] // Offside.kz. URL: https://offside.kz/avto/28575-shtraf-za-telefon-s-kamery-sergek-kak-dokazat-svoiu-pravotu-i-obzhalovat-predpisanie (дата обращения: 27.08.2026).

9. Этика и лучшие практики ИИ в распознавании лиц [Электронный ресурс] // Didit. URL: https://didit.me/ru/blog/the-ethics-and-best-practices-of-ai-in-facial-recognition/ (дата обращения: 27.08.2026).

10. Конституция Республики Казахстан (принята на референдуме 15 марта 2026 г.) [Электронный ресурс] // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/K2600000000 (дата обращения: 27.08.2026).

11. О мерах по реализации законов Республики Казахстан от 17 ноября 2025 года «Об искусственном интеллекте» и «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации»: распоряжение Премьер-Министра Республики Казахстан от 14 января 2026 года № 2-р [Электронный ресурс] // ИПС «Әділет». URL: https://adilet.zan.kz/rus/docs/R2600000002 (дата обращения: 27.08.2026).

12. Новые штрафы за незаконное использование искусственного интеллекта появятся в Казахстане [Электронный ресурс] // Zakon.kz. URL: https://www.zakon.kz/pravo/6504703 (дата обращения: 27.08.2026).

13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union, L, 12.07.2024. // https://eur-lex.europa.eu/eli/reg/2024/1689/oj

КРАВЦОВА ЮЛИЯ АНАТОЛЬЕВНА
Начальник кафедры психологии и педагогики
Воронежского института МВД России
кандидат психологических наук, доцент
полковник полиции

ЭТИКА ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. *Статья посвящена этическим аспектам применения искусственного интеллекта в правоохранительных органах. Рассматриваются проблемы цифровой этики, включая феномен «черного ящика», вопросы обеспечения корректности работы систем искусственного интеллекта и защиты конфиденциальности граждан. Обосновывается важность соблюдения этических принципов и сохранения ведущей роли человека в цифровизируемой сфере обеспечения правопорядка.*

Ключевые слова: *искусственный интеллект, цифровой гуманизм, профессиональная этика, правоохранительные органы, интеллектуальное иждивенчество, распределенное познание, критическое мышление, подготовка курсантов, эффект «черного ящика».*

Современная деятельность сотрудников правоохранительных органов претерпевает радикальные изменения под влиянием цифровизации, и ключевым технологическим фактором этого процесса становится искусственный интеллект (ИИ).

Широкое внедрение систем ИИ в деятельность правоохранительных органов обычно оценивается сквозь призму технологической и прагматической эффективности. Алгоритмы прогностического моделирования криминогенной обстановки, системы распознавания образов и автоматизированный анализ больших данных прочно вошли в практику ведомственных структур. Сегодня эти технологии выполняют роль важнейших аналитических инструментов. В качестве иллюстрации обратимся к прогностическим алгоритмам. Оценка статистических данных позволяет ИИ определять вероятность правонарушений на конкретных городских участках, что может обусловливать распределение патрульных экипажей. Сходным образом действуют технологии распознавания образов и биометрии: автоматическая обработка видеопотока обеспечивает выявление разыскиваемых лиц непосредственно в людных местах. Параллельно с этим методы анализа больших данных ускоряют поиск скрытых зависимостей в массивах информации. На основе сопоставления деталей различных уголовных дел, финансовых транзакций и цифровых следов алгоритмы обнаруживают связи, которые ранее требовали длительной аналитической работы [1].

Однако технические возможности ИИ порождают целый комплекс этических проблем, которые невозможно решить исключительно нормативными методами. Профессиональная этика сотрудника правоохранительных органов сталкивается с новыми вызовами, требующими переосмысления традиционных принципов

деятельности специалиста. Специфика правоохранительной сферы заключается в том, что принимаемые здесь решения непосредственно затрагивают свободу, законные интересы и достоинство личности. Когда мы перекладываем когнитивные функции на автоматические системы, профессиональное мышление, строго говоря, меняет свою природу. Отсюда и возникает, на наш взгляд, острая необходимость как можно точнее очертить этические рамки применения подобных технологий. Без таких барьеров техническое содействие рискует обернуться, если можно так выразиться, полной утратой эмпатии и, как следствие, самого чувства справедливости у сотрудников.

Вообще вопрос человеческой эмпатии занимает особое место в этике применения искусственного интеллекта. Данное качество является фундаментом юридической профессии и по своей природе недоступно никаким вычислительным системам. Искусственный интеллект способен анализировать данные, выявлять закономерности, прогнозировать вероятности, но он не способен сопереживать, ощущать эмоциональную сторону человеческих переживаний, учитывать моральную сложность жизненных ситуаций. Правоохранитель, напротив, действует не только как специалист, но и как человек, обладающий способностью к нравственному осмыслению последствий своих решений. Именно эмпатия позволяет специалисту учитывать тончайшие нюансы дела: страхи подсудимого, уязвимость потерпевшего, мотивацию участников конфликта и их внутренние переживания — все то, что невозможно выразить исключительно в числовых параметрах или текстовых данных.

В целом концепция цифрового гуманизма предполагает, что любые технологии должны выступать лишь средством расширения человеческих возможностей, не снимая с субъекта моральной ответственности. Внедрение подобных стандартов призвано сберечь этическую основу деятельности правоохранителя и удержать искусственный интеллект в статусе ассистента, а не замены специалиста.

Ряд исследователей, изучающих вопросы использования ИИ в правоохранительной деятельности, обращает внимание на риски, связанные с изменением внутренней установки сотрудника при работе с ним [2, 3, 4]. Получая от программы готовый аналитический вывод или рекомендацию (например, о высокой степени криминогенности конкретного лица или территории), правоохранитель подсознательно склонен соглашаться с машиной, ослабляя собственный критический анализ. Происходит психологическое замещение профессиональной интуиции и опыта сухим математическим расчетом. С этической точки зрения это ведет к постепенной потере субъектности: человек превращается в исполнителя воли алгоритма, что размывает понятие личной моральной ответственности за итоговый результат.

Особое значение эта когнитивная деформация приобретает в процессе профессиональной подготовки и обучения курсантов ведомственных образовательных организаций. Сегодня будущие специалисты правоохранительных органов активно используют генеративные технологии ИИ для решения учебных задач: от написания рефератов до автоматического моделирования планов расследования в рамках практических занятий. С точки зрения образовательной

этики бесконтрольное применение подобных инструментов на этапе формирования профессионала несет в себе скрытую угрозу. Отметим, что привычка решать учебные задачи простым заимствованием результатов работы нейросети напрямую тормозит формирование критического мышления и профессиональной ответственности. Когда курсант выбирает быстрый и внешне безупречный ответ машины, постепенно атрофируется навык самостоятельного поиска решения.

Кроме того, слепое использование ИИ в учебном процессе приводит к профессиональной инфантильности. Специалист, привыкший к тому, что интеллектуальная система «все делает за него», не сможет эффективно работать в реальных условиях. Никакая искусственная интеллектуальная система не заменит личного опыта, умения формировать правовую аргументацию и способности противостоять оппоненту в ходе проблемной профессиональной ситуации. Как отмечают Миронова Е.А. и Миниязова А.И. в профессиональном сообществе растет обеспокоенность тем, что чрезмерная автоматизация обучения приведет к появлению специалистов нового типа, которые формально имеют диплом, но, по сути, не обладают навыками профессионального мышления. Подобная тенденция может нанести урон не только качеству деятельности, но и будущему всей правоохранительной системы, поскольку она строится на компетентности, ответственности и зрелости профессионала [5].

Именно поэтому исследователи подчеркивают необходимость предотвращения подобного «интеллектуального иждивенчества», что требует кардинального пересмотра подходов к профессиональному обучению. Будущих специалистов необходимо целенаправленно учить не пассивному потреблению готовых выводов машины, а их критическому и всестороннему осмыслению. Сотрудник органов правопорядка обязан четко видеть границы применимости технологий и своевременно распознавать системные сбои в данных. Искусственный интеллект — это всего лишь ассистент, а вовсе не полноценная замена человеку. Именно эта мысль должна стать фундаментом профессионального взгляда сотрудника правоохранительных органов. Только тогда, и никак иначе, молодой специалист получит шанс применять цифровые инструменты осмысленно. Это позволит ему, строго говоря, оставаться самостоятельным, морально и этически ответственным субъектом в своей профессии.

Если оставить в стороне риски обучения, то главным препятствием становится сама специфика нейросетевых моделей. Речь идет о так называемой «проблеме черного ящика», что означает полную закрытость системы, когда сотрудник никак не может проследить, как именно машина анализировала данные. Если технология выносит вердикт, но скрывает понятные критерии, ее использование, на наш взгляд, прямо противоречит самому духу деятельности правоохранительных органов. Ведь базовый этический стандарт требует главного — чтобы за любым решением правоохранителя стояли аргументы, которые можно проверить извне. А специалист нередко оказывается в положении, когда он вынужден полагаться на итоговый результат, внутреннюю суть которого сам не может до конца осмыслить.

Взаимодействие с системами «черного ящика» таит в себе опасность психологической деформации сотрудника. Под влиянием технологий понимание

справедливости рискует сместиться от живого сопереживания и погружения в человеческую драму к сугубо механистической позиции. Это грозит жесткой формализацией правоохранительной сферы, когда вместо детального анализа конкретной ситуации на первый план выходят расчеты, подготовленные ИИ. При подобной подмене гражданин, нуждающийся в защите, лишается возможности полноценного диалога с мыслящим и сопереживающим человеком.

Масштабное использование автоматизированных систем для мониторинга информационных потоков, пространственных и биометрических данных существенно переформатирует современные представления об общественной безопасности. В этих реалиях классическая защита прав граждан неизбежно дополняется необходимостью обеспечения цифровой приватности. Профессиональная этика буквально заставляет нас искать хрупкое равновесие: сбор сведений не должен подрывать общественное доверие. Важно, строго говоря, превратить технологии в элемент защиты, убрав из них маркеры скрытого социального давления. В итоге этический вектор правоохранительных органов смещается к защите личных границ человека, где любые служебные задачи выполняются без ущемления его фундаментальных свобод [6].

Осознание тех пределов, за которыми любое вторжение в частную жизнь гражданина становится избыточным, — это, строго говоря, базис служебной этики. Когда алгоритмические системы пытаются превентивно просчитывать поведение людей, под удар неизбежно попадает хрупкое равновесие между охраной правопорядка и уважением к человеку. С этических позиций цифрового гуманизма внутреннее благополучие гражданина и его право на приватность, как нам кажется, безоговорочно важнее технологической целесообразности. Из этого следует лишь одно: обращение к подобным инструментам требует жестких рамок конкретных задач, а сами персональные данные должны лишаться любых идентификационных признаков.

В этой ситуации внешние правовые ограничения отступают на второй план, ведь этика применения ИИ во многом зависит от внутренней культуры самого сотрудника. Без осознанного отказа от «интеллектуального иждивенчества» ответственная работа с технологиями попросту невозможна. Профессионал не уступает свои мыслительные функции компьютеру. Скорее, речь идет о содержательном диалоге с цифровым ассистентом. Алгоритмам делегируется техническая рутина — поиск по базам данных, сверка статистических показателей и сортировка документов. Подобное взаимодействие, очевидно, укладывается в концепцию распределенного познания. Машина расширяет аналитический потенциал человека, но право финального выбора всегда сохраняется за специалистом.

Понимание глубинного смысла ситуации и принятие решений — это то, что всегда остается прерогативой человека, какие бы технологии ни использовались. Правоохранитель не может слепо полагаться на логику программных продуктов. Каждая рекомендация ИИ должна, строго говоря, фильтроваться через внутренние ценности специалиста: его моральный опыт, честность и сострадание к гражданам. Подобное отношение к делу защищает сотрудника от превращения в механического исполнителя воли алгоритма. При таком распределении ролей искусственный

интеллект органично встраивается в систему, становясь полезным, честным и абсолютно подконтрольным человеку помощником.

Подводя итоги, важно подчеркнуть: цифровая модернизация органов правопорядка отчетливо доказывает, что развитие морально-этических стандартов должно опережать технологический прогресс. Чтобы защитить идеалы цифрового гуманизма и не допустить деформации сознания сотрудников, необходимо сосредоточиться на решении конкретных практических задач:

- обеспечении когнитивной автономии специалиста. Ведомственные методики подготовки кадров, на наш взгляд, следует ориентировать на формирование глубокого критического мышления. Только такой подход поможет будущим специалистам взвешенно анализировать поступающие данные и успешно противостоять эффекту «интеллектуального иждивенчества»;

- внедрение системы нормативно-организационного контроля и этической экспертизы. Программные комплексы и интеллектуальные системы, внедряемые в практику правоохранительных органов, должны, строго говоря, проходить обязательный междисциплинарный аудит гуманитарной направленности. Подобные превентивные меры необходимы, на наш взгляд, для своевременного обнаружения и устранения скрытых дефектов — тех самых изъянов, которые легко могут привести к предвзятым либо ошибочным выводам при анализе массивов данных. Кроме того, предварительная экспертиза позволяет очертить четкие границы использования технологий. Это исключает риск перекладывания моральной ответственности сотрудников на автоматизированные выводы систем. В данном контексте ключевым условием выступает сохранение приоритета человека;

- признание ведущей роли человека как субъекта принятия решений. В профессиональной этике важно закрепить статус искусственного интеллекта как исключительно вспомогательного средства. Смысловой анализ ситуации, искреннее сопереживание личности и принятие окончательного решения должны оставаться безусловным правом и обязанностью человеческого сознания.

Завершая рассмотрение данной темы, можно сделать вывод, что успешная интеграция искусственного интеллекта в правоохранительную деятельность требует совместных усилий технических экспертов, юристов, экспертов по этике и общества в целом. Только при соблюдении баланса между инновациями и этикой можно в полной мере реализовать потенциал искусственного интеллекта в правоохранительных органах.

Список литературы:

1. Селимова А. М. Внедрение искусственного интеллекта в правоохранительную сферу / А. М. Селимова, Ш. Я. Исаков // Human Progress. —– 2024. — Том 10. — Вып. 10. — С. 31—35.

2. Воробьева Е. А. Этические аспекты использования систем искусственного интеллекта при расследовании преступлений / Е. А. Воробьева // Вестник Саратовской государственной юридической академии. — 2022. — № 4 (147). — С. 162—172.

3. Закурдаев Д. А. Применение искусственного интеллекта в судебной, правоохранительной и адвокатской деятельности: возможности, этические аспекты и проблемы / Д. А. Закурдаев // Молодой ученый. — 2024. — № 2 (501). — С. 193—196.

4. Саранцева С. Г. Искусственный интеллект в юриспруденции: современные методы и интеграция с правовыми теориями / С. Г. Саранцев // Закон и право. — 2025. — №6. — С. 188—192.

5. Миронова Е. А. Этика использования искусственного интеллекта в профессиональной деятельности юриста / Е. А. Миронова, А. И. Миниязова // Научные исследования 2025 : сборник статей XIX Международной научно-практической конференции. — Пенза: Наука и Просвещение, 2025. — С. 123—128.

6. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы : монография / Д. В. Бахтеев .— Москва : Проспект, 2021 .— 176 с.

КУСАИНОВА АЛИЯ МАРАТОВНА
докторант 2 курса Академии управления
МВД Республики Казахстан
магистр права, подполковник полиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИССЛЕДОВАНИИ И ЦИФРОВОЙ РЕКОНСТРУКЦИИ СЛЕДОВ СОЗДАНИЯ ПОМЕХ УПРАВЛЕНИЮ ВОЗДУШНЫМ СУДНОМ

Современная авиационная деятельность характеризуется высокой степенью цифровизации. Управление воздушным движением, навигация, регистрация параметров полета, функционирование бортовых систем, радиосвязь и различные элементы обеспечения безопасности сопровождаются формированием значительного массива цифровой информации. В результате авиационное происшествие или инцидент может оставлять не только традиционные материальные и документальные следы, но и сложный комплекс цифровых следов, распределенных между различными техническими системами.

Особую сложность представляют ситуации, связанные с созданием помех управлению воздушным судном. В таких случаях необходимо установить не только факт воздействия, но и его характер, временной момент, пространственное положение источника воздействия, механизм влияния на воздушное судно и экипаж, возникшие последствия, а также взаимосвязь между отдельными элементами события.

Для уголовного судопроизводства принципиальное значение имеет переход от разрозненных сведений к доказательственно значимой реконструкции события. Именно здесь технологии искусственного интеллекта способны выполнять вспомогательную аналитическую функцию.

Международная авиационная практика рассматривает искусственный интеллект как перспективный инструмент повышения безопасности полетов, оптимизации процессов и анализа больших массивов авиационных данных [1]. Европейское агентство по безопасности полетов отмечает потенциал искусственного интеллекта для повышения эффективности управления безопасностью, выявления уязвимостей и возникающих рисков, а также классификации и приоритизации проблем безопасности. Вместе с тем подчеркивается необходимость обеспечения доверенности и надежности ИИ-систем, включая контроль качества данных и процесса машинного обучения, валидацию результатов, объяснимость алгоритмов, надлежащее управление данными и учет этических аспектов их применения [2].

Таким образом, применительно к расследованию создания помех управлению воздушным судном возникает научная задача формирования методики, позволяющей использовать возможности искусственного интеллекта без подмены им следователя или эксперта.

Создание помех управлению воздушным судном представляет собой событие, которое может проявляться одновременно в нескольких информационных средах. В зависимости от конкретного механизма воздействия следы могут

фиксироваться в бортовых системах воздушного судна, средствах объективного контроля, системах наблюдения, радиопереговорах, диспетчерских системах, навигационных данных, видеозаписях, показаниях членов экипажа и иных источниках [3].

В связи с этим целесообразно рассматривать цифровой след не как отдельный файл или запись, а как информационный элемент, содержащий сведения о факте, времени, месте, механизме либо последствиях исследуемого события.

Особое значение имеет корреляция нескольких независимых источников. Например, сведения бортовой регистрации могут сопоставляться с данными диспетчерской службы, радиопереговорами, координатами воздушного судна, метеорологической информацией, видеозаписями и показаниями экипажа. При совпадении временных параметров и согласованности пространственных характеристик появляется возможность построения единой модели события.

Именно на этом этапе применение ИИ может существенно повысить эффективность исследования.

Искусственный интеллект целесообразно рассматривать не как самостоятельный источник доказательства, а как технологический инструмент обработки и анализа уже полученной информации [4].

Одним из более перспективных направлений является автоматизированная обработка больших массивов разнородных данных. Алгоритмы машинного обучения способны выявлять закономерности и корреляции, которые трудно обнаружить при последовательном ручном изучении большого количества записей.

В рамках расследования создания помех управлению воздушным судном применение технологий искусственного интеллекта может быть ориентировано на комплексный анализ разнородных цифровых следов и установление взаимосвязи между ними.

ИИ может использоваться для автоматизированного распределения поступающей информации по типам и источникам: данным бортовых систем, радиопереговорам, видеозаписям, координатам, сведениям о функционировании технических средств, показаниям участников события и иным материалам. Это позволяет систематизировать значительный объем разнородной информации и подготовить его для последующего анализа.

При расследовании авиационных инцидентов сведения могут поступать из источников, функционирующих с различными временными параметрами. ИИ-инструменты могут применяться для сопоставления временных меток, выявления последовательности действий и формирования единой хронологии развития события.

Алгоритмический анализ позволяет выявлять статистические и временные взаимосвязи между изменениями параметров полета, действиями экипажа, радиопереговорами, командами диспетчера, функционированием бортовых систем и иными зафиксированными обстоятельствами. Полученные взаимосвязи могут использоваться для формирования и проверки следственных версий.

Обработка координат, данных о траектории движения и иных геопространственных параметров позволяет определить взаимное положение воздушного судна, предполагаемого источника воздействия и объектов

окружающей обстановки. Результатом может выступать цифровая пространственная модель, позволяющая визуализировать механизм события.

Наиболее комплексным направлением является интеграция временных, пространственных и содержательных характеристик цифровых следов в единую модель события [5]. Такая реконструкция позволяет воспроизвести предполагаемую последовательность действий, определить взаимное положение объектов и сопоставить различные источники информации, сформировав целостное представление о механизме создания помех управлению воздушным судном.

Современные исследования подтверждают перспективность ИИ для анализа авиационных происшествий [6]. В частности, исследования 2025–2026 гг. демонстрируют применение больших языковых моделей, графов знаний и гибридных ИИ-моделей для извлечения событий, построения причинно-следственных связей и анализа авиационных отчетов [7].

При этом использование ИИ в авиационной сфере сопровождается принципиальным требованием доверия к результатам. Европейское агентство по безопасности полетов выделяет такие проблемы, как качество и репрезентативность данных, устойчивость моделей, объяснимость и неопределенность результатов.

Следовательно, эти требования должны учитываться и при криминалистическом применении ИИ.

В международной авиационной практике расследование авиационных происшествий и инцидентов основывается на систематическом исследовании фактических обстоятельств, технических данных и иных материалов, имеющих значение для установления причин и обстоятельств авиационного события [8]. Основополагающие международные стандарты и рекомендуемая практика в данной сфере закреплены в Приложении 13 к Конвенции о международной гражданской авиации «Расследование авиационных происшествий и инцидентов» [9]. Методические аспекты проведения расследования конкретизированы в Руководстве по расследованию авиационных происшествий и инцидентов, предусматривающем исследование воздушного судна, его конструкций и систем, бортовых регистраторов, характеристик воздушного судна и других материалов, необходимых для установления обстоятельств и причин происшествия [8].

Следовательно, использование ИИ целесообразно интегрировать именно в существующую систему исследования, а не противопоставлять традиционным методам.

Искусственный интеллект способен стать эффективным инструментом криминалистического исследования цифровых следов создания помех управлению воздушным судном. Его основное значение заключается не в автоматическом установлении виновности либо формировании готового доказательства, а в повышении возможностей следователя и эксперта по обработке больших объемов разнородной информации.

Научно обоснованное применение ИИ позволяет перейти от анализа отдельных цифровых следов к их системной корреляции и пространственно-временной реконструкции события. В результате появляется возможность сформировать единую цифровую модель, отражающую последовательность

событий, положение воздушного судна, временные параметры воздействия, изменение характеристик полета и возможные последствия.

Разработка такой системы может стать одним из элементов цифровой трансформации криминалистического обеспечения расследования преступлений против безопасности движения и эксплуатации воздушного транспорта и одновременно обеспечить научно обоснованный переход от фрагментарного исследования цифровых следов к комплексной реконструкции механизма противоправного воздействия.

Список литературы:

1. International Civil Aviation Organization. Using artificial intelligence to improve global aviation safety [Электронный ресурс]. -URL: https://www.icao.int/sites/default/files/Meetings/a41/Documents/WP/wp_090_en.pdf?utm_source.

2. European Union Aviation Safety Agency (EASA). Artificial Intelligence Roadmap 2.0: A human-centric approach to AI in aviation [Электронный ресурс]. -Cologne: EASA, 2023. -URL: https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20 (дата обращения: 14.09.2026).

3. Baibussinov A., Shayakhmetov M., Rzayeva L., Yesbergenov K. A Hardware-Software Complex for the Reconstruction of Unmanned Aerial Vehicle Digital Traces Under Logical Data Damage Using LSTM-Based Telemetry Recovery and Multi-Source Confidence Scoring // Journal of Cybersecurity and Privacy. -2026. -Vol. 6, No. 4. -Art. 123. -DOI: 10.3390/jcp6040123.

4. European Commission. AI Act Service Desk. Law Enforcement [Электронный ресурс]. -URL: https://ai-act-service-desk.ec.europa.eu/en/law-enforcement?utm_source.

5. Lin H., Zhang J., Yao X., Guo D. AI4AirSafe: A Quintuple KG–LLM Framework for Causal Reasoning in Aviation Accidents // Journal of Safety Science and Resilience. -2026. -Art. 100331. -DOI: 10.1016/j.jnlssr.2026.100331.

6. Liu Q., Li F., Ng K. K. H., Han J., Feng S. Accident investigation via LLMs reasoning: HFACS-guided Chain-of-Thoughts enhance general aviation safety // Expert Systems with Applications. -2025. -Vol. 269. -Art. 126422. -DOI: 10.1016/j.eswa.2025.126422.

7. Lin H., Zhang J., Yao X., Guo D. AI4AirSafe: A Quintuple KG–LLM Framework for Causal Reasoning in Aviation Accidents // Journal of Safety Science and Resilience. 2026. DOI: 10.1016/j.jnlssr.2026.100331.

8. International Civil Aviation Organization. Manual of Aircraft Accident and Incident Investigation. Part III — Investigation (Doc 9756) [Электронный ресурс]. — 2nd ed. — Montréal : International Civil Aviation Organization, 2024. — 628 p. — URL: https://store.icao.int/en/manual-of-aircraft-accident-and-incident-investigation-part-iii-investigation-doc-9756-part-3.

9. Международная организация гражданской авиации (ИКАО). Приложение 13 к Конвенции о международной гражданской авиации. Расследование авиационных происшествий и инцидентов: международные стандарты и рекомендуемая практика [Электронный ресурс]. 12-е изд. Монреаль : ИКАО. -URL: https://www.icao.int/safety/AIG/Pages/Annex-13.aspx (дата обращения: 14.09.2026).

КУШЕНОВ АЙСАТ МАРАТОВИЧ
Магистрант Актюбинского юридического института
МВД Республики Казахстан имени М.Букенбаева
старший лейтенант полиции

ПРЕДИКТИВНЫЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОФИЛАКТИКЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА И ДРОППЕРСТВА СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ В РЕСПУБЛИКЕ КАЗАХСТАН

В настоящее время актуальность применения предиктивных технологий искусственного интеллекта в профилактике интернет-мошенничества и дропперства среди несовершеннолетних в Республике Казахстан обусловлена не только стремительным развитием цифровой среды, но и устойчивой динамикой совершаемых с ее использованием преступлений. Цифровизация финансовых отношений, широкое распространение мобильных банковских приложений, социальных сетей и мессенджеров создали новые возможности для преступников, которые все чаще используют дистанционные способы воздействия на граждан. Особую обеспокоенность в данном направлении вызывает вовлечение несовершеннолетних в противоправные схемы, поскольку подростки в силу возраста, недостаточного опыта и стремления к получению быстрого заработка могут становиться объектами манипуляции со стороны организаторов преступной деятельности.

Статистические данные подтверждают необходимость усиления профилактического направления. Согласно данным Генеральной прокуратуры Республики Казахстан, в 2022 году было зарегистрировано 20 569 фактов интернет-мошенничества, в 2023 году данный показатель увеличился до 21 777 фактов, а в 2024 году достиг 22 870 фактов [1]. Так, за рассматриваемый период наблюдается устойчивая тенденция роста интернет-мошенничества, несмотря на снижение общего количества зарегистрированных уголовных правонарушений. В частности, в 2024 году их общее количество снизилось на 5% – со 140 272 до 132 778, тогда как число интернет-мошенничеств, напротив, увеличилось на 5% [1].

Ситуация сохраняла напряженный характер и в 2025 году. За первое полугодие 2025 года в Республике Казахстан было зарегистрировано 12 390 фактов интернет-мошенничества против 9 936 за аналогичный период 2024 года, что свидетельствует о росте примерно на 24,7%. За этот период от действий интернет-мошенников пострадали почти 23 тыс. граждан, а причиненный ущерб превысил 25 млрд тенге [2]. Представленные данные позволяют сделать вывод о сохранении высокого уровня цифровой преступности и необходимости совершенствования механизмов ее раннего предупреждения.

Особую актуальность проблема приобретает в отношении несовершеннолетних. По данным Бюро национальной статистики Республики Казахстан, количество зарегистрированных преступлений, совершенных несовершеннолетними или при их соучастии, составило 1 735 в 2022 году, 1 925 в 2023 году, 1 890 в 2024 году и 2 461 в 2025 году [3]. При этом в 2025 году по

сравнению с 2024 годом количество таких преступлений увеличилось примерно на 30,2%. Вместе с тем приведенные показатели характеризуют подростковую преступность в целом и не позволяют непосредственно определить количество несовершеннолетних, вовлеченных именно в интернет-мошенничество или дропперство. Безусловно, данная статистика подтверждает необходимость усиления профилактической работы с несовершеннолетними в условиях расширения цифровой среды. При этом современная цифровизация обусловливает не только увеличение масштабов интернет-мошенничества, но и изменение способов вовлечения несовершеннолетних в противоправную деятельность.

Одним из наиболее опасных направлений является вовлечение подростков в дропперские схемы под видом легального заработка. Несовершеннолетнему может предлагаться вознаграждение за предоставление банковской карты, получение денежных средств и их последующий перевод на указанные счета. При этом подросток не всегда осознает противоправный характер своих действий и может рассматривать их исключительно как способ получения дополнительного дохода.

В связи с повышением общественной опасности данного явления в Казахстане с 16 сентября 2025 года введена уголовная ответственность за дропперство. Соответствующие положения закреплены в статье 232-1 Уголовного кодекса Республики Казахстан, предусматривающей ответственность за незаконное предоставление, передачу и приобретение доступа к банковскому счету, платежному инструменту или идентификационному средству, а также за незаконное осуществление платежей и переводов денег [4]. Появление специальной уголовно-правовой нормы свидетельствует о необходимости формирования комплексной системы противодействия дропперству, включающей не только уголовно-правовые меры, но и инструменты ранней профилактики.

Важным направлением совершенствования данной профилактики является использование технологий искусственного интеллекта. Предиктивные алгоритмы способны анализировать большие массивы цифровых данных и выявлять совокупность признаков, характерных для мошеннических схем. В частности, алгоритмы машинного обучения могут использоваться для выявления подозрительных финансовых операций, анализа цифровых коммуникаций, обнаружения повторяющихся моделей поведения и установления взаимосвязей между различными аккаунтами и платежными инструментами.

Перспективным является применение технологий обработки естественного языка для выявления характерных способов вербовки несовершеннолетних. Анализ сообщений в цифровой среде может позволить выявлять предложения о «легком заработке», просьбы предоставить банковскую карту или счет, предложения получить процент за перевод денежных средств и другие типовые признаки вовлечения подростков в дропперскую деятельность. При этом алгоритм должен оценивать не отдельное слово или сообщение, а совокупность взаимосвязанных признаков, что позволит снизить количество ошибочных срабатываний.

Практическая необходимость применения таких технологий подтверждается развитием в Казахстане финансовой инфраструктуры противодействия мошенничеству. В 2024 году на базе Национального Банка Республики Казахстан был создан Антифрод-центр, предназначенный для обмена информацией между

финансовыми организациями и правоохранительными органами и оперативного реагирования на подозрительные операции [5, 6]. Дальнейшее развитие данной системы с использованием технологий искусственного интеллекта может обеспечить переход от обнаружения уже совершенных подозрительных операций к прогнозированию потенциальных рисков.

Вместе с тем применение предиктивных технологий в отношении несовершеннолетних требует соблюдения правовых и этических гарантий. Результат работы алгоритма не должен рассматриваться как доказательство виновности лица. Искусственный интеллект может определить повышенную вероятность возникновения определенного риска, однако окончательная правовая оценка должна осуществляться уполномоченным сотрудником. Особенно важно обеспечить защиту несовершеннолетних от ошибочной классификации, поскольку наличие определенных цифровых или финансовых признаков само по себе не свидетельствует о совершении преступления.

В связи с этим особое значение приобретает вопрос практического внедрения технологий искусственного интеллекта непосредственно в деятельность правоохранительных органов. Современные условия цифровой трансформации требуют совершенствования не только технических средств выявления преступлений, но и самого подхода к организации профилактической работы. Если традиционные методы в значительной степени ориентированы на реагирование после совершения противоправного деяния, то использование предиктивных технологий позволяет сформировать более превентивную модель, при которой внимание правоохранительных органов сосредоточивается на выявлении факторов и обстоятельств, способствующих совершению преступления.

Применительно к интернет-мошенничеству и дропперству среди несовершеннолетних, такая модель приобретает особую значимость, поскольку вовлечение подростка в преступную схему, как правило, начинается задолго до момента совершения конкретной финансовой операции. Первоначально происходит установление контакта, формирование доверия, предложение материального вознаграждения и постепенное убеждение несовершеннолетнего в том, что предлагаемые действия являются законными. Следовательно, профилактическое воздействие наиболее эффективно именно на ранних этапах, когда подросток еще не совершил противоправного действия и может быть выведен из ситуации риска.

Внедрение искусственного интеллекта в деятельность правоохранительных органов в данном случае должно быть направлено прежде всего на обеспечение своевременного выявления подобных ситуаций. Обработка значительных объемов цифровой информации позволяет устанавливать повторяющиеся признаки мошеннических схем и выявлять взаимосвязь между различными событиями, которые при обычном анализе могут рассматриваться как не связанные между собой. Например, отдельное предложение о получении заработка за использование банковской карты может не свидетельствовать о преступлении, однако его сочетание с другими признаками – характером коммуникации, повторяемостью аналогичных предложений, связью с подозрительными аккаунтами и

последующими финансовыми операциями, может указывать на формирование дропперской схемы.

Так, значение искусственного интеллекта заключается не столько в автоматическом обнаружении самого преступления, сколько в способности своевременно обратить внимание на совокупность обстоятельств, которые могут предшествовать его совершению. Данное обстоятельство позволяет изменить характер деятельности правоохранительных органов, от фиксации последствий преступной деятельности к предупреждению ее развития. При этом технологический инструмент должен дополнять профессиональную деятельность сотрудника, а не заменять ее.

Особенно важно учитывать данное обстоятельство при работе с несовершеннолетними. Подросток, оказавшийся в поле внимания правоохранительных органов вследствие выявленных алгоритмом признаков риска, не должен автоматически рассматриваться как лицо, склонное к совершению преступления. В ряде случаев он может быть жертвой психологического воздействия, обмана или манипуляции со стороны взрослых участников преступной схемы. Поэтому результаты интеллектуального анализа должны служить основанием для более внимательного изучения ситуации и выбора соответствующей профилактической меры, а не для автоматического применения мер уголовно-правового характера.

Указанный подход предполагает изменение и организационной структуры профилактической деятельности. Внедрение искусственного интеллекта требует определения порядка получения, обработки и передачи информации, а также четкого разграничения ответственности между техническими специалистами, аналитиками и сотрудниками правоохранительных органов. Результат автоматизированного анализа должен поступать к уполномоченному сотруднику в форме аналитической информации, позволяющей оценить степень риска и определить дальнейшие действия. При этом каждое решение, способное затронуть права несовершеннолетнего, должно приниматься человеком с учетом конкретных обстоятельств ситуации.

Необходимость человеческого контроля обусловлена и тем, что предиктивная модель не обладает абсолютной точностью. Любой алгоритм может ошибочно определить обычное поведение как подозрительное либо, напротив, не распознать новую разновидность мошеннической схемы. Поэтому внедрение искусственного интеллекта должно сопровождаться постоянным анализом результатов его работы, выявлением ошибок и корректировкой используемых моделей. Чем выше потенциальные последствия принятого решения, тем более значимой становится необходимость его дополнительной проверки специалистом.

Одновременно внедрение интеллектуальных технологий предполагает развитие межведомственного взаимодействия. Интернет-мошенничество и дропперство не ограничиваются сферой деятельности одного государственного органа, поскольку соответствующие схемы затрагивают финансовую систему, информационное пространство и сферу профилактики правонарушений среди несовершеннолетних.

В связи с этим эффективная профилактическая модель должна предусматривать взаимодействие правоохранительных органов с финансовыми организациями, образовательными учреждениями и иными субъектами профилактики.

Особое место в данной системе занимает и финансовый сектор. Именно через банковские счета, платежные карты и иные финансовые инструменты осуществляется значительная часть операций, связанных с дропперскими схемами. Поэтому объединение возможностей финансового мониторинга и предиктивной аналитики правоохранительных органов способно существенно повысить эффективность выявления подозрительных цепочек переводов. При этом речь должна идти не о передаче неограниченного объема информации, а о законном и целевом обмене сведениями, необходимыми для предупреждения конкретных угроз.

Не менее важным является взаимодействие с образовательными организациями. Поскольку значительная часть вовлечения подростков осуществляется посредством интернет-платформ, профилактическая работа должна начинаться еще до возникновения непосредственного контакта с преступниками. Результаты анализа распространенных мошеннических сценариев могут использоваться для разработки образовательных материалов и практических программ по цифровой и финансовой грамотности. Подросткам необходимо объяснять не только общие правила безопасного поведения в интернете, но и конкретные признаки предложений, связанных с незаконным использованием банковских счетов и платежных инструментов.

В таком понимании искусственный интеллект становится одним из элементов единой системы профилактики, объединяющей технологические и социальные механизмы. Он позволяет обрабатывать информацию и выявлять потенциальные угрозы, правоохранительные органы обеспечивают правовую оценку и реагирование, образовательные организации осуществляют профилактическую работу, а финансовые учреждения способствуют своевременному выявлению подозрительных операций. Результатом такого взаимодействия должно стать не увеличение числа привлеченных к ответственности несовершеннолетних, а снижение количества случаев их вовлечения в преступные схемы.

При этом дальнейшее развитие предиктивных технологий в правоохранительной сфере должно сопровождаться совершенствованием нормативного регулирования. Необходимо четко определить цели и пределы использования алгоритмических систем, порядок обработки информации, требования к защите персональных данных, условия хранения результатов анализа и ответственность за неправомерное использование полученной информации. Особого внимания требуют сведения, относящиеся к несовершеннолетним, поскольку их обработка предполагает повышенный уровень защиты и недопущение необоснованного вмешательства в частную жизнь.

В конечном счете эффективность внедрения искусственного интеллекта определяется не только техническими возможностями алгоритмов, но и тем, насколько грамотно они встроены в существующую систему профилактики. Технология сама по себе не способна устранить причины интернет-мошенничества

или дропперства. Однако она может существенно повысить способность правоохранительных органов своевременно обнаруживать изменения в преступной среде, устанавливать взаимосвязи между отдельными событиями и концентрировать профилактические ресурсы там, где вероятность возникновения угрозы является наиболее высокой.

Следовательно, внедрение искусственного интеллекта в деятельность правоохранительных органов Республики Казахстан целесообразно рассматривать как переход к качественно иной организации профилактической работы, основанной на своевременном выявлении риска, его оценке и принятии адресных мер реагирования.

В отношении несовершеннолетних такой подход особенно важен, поскольку позволяет сместить акцент с последующего наказания на предупреждение вовлечения подростка в противоправную деятельность. Именно в этом заключается основное профилактическое значение предиктивных технологий, они должны помогать правоохранительной системе не только устанавливать факт уже совершенного преступления, но и своевременно предотвращать ситуацию, которая может привести к его совершению.

Список литературы:

1. Генеральная прокуратура Республики Казахстан. О криминогенной ситуации за 2024 год [Электронный ресурс]. – 2025. – Режим доступа: https://www.gov.kz/memleket/entities/prokuror/press/article/details/192800?lang=ru. – Дата обращения: 26.08.2026.

2. Генеральная прокуратура Республики Казахстан. Данные о состоянии интернет-мошенничества за первое полугодие 2025 года [Электронный ресурс]. — 2025. — Режим доступа: https://taspanews.kz/novosti-kazakhstana/kolichestvo-prestupleniy-za-pervoe-polugodie-2025-statistika-genprokuratury-774851144981/ – Дата обращения: 26.08.2026.

3. Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан. Преступность несовершеннолетних по отдельным видам преступлений [Электронный ресурс]. — Режим доступа: https://bala.stat.gov.kz/prestupnost-nesovershennoletnih-po-otdelnym-vidam-prestuplenij/ – Дата обращения: 26.08.2026.

4. Генеральная прокуратура Республики Казахстан. В Казахстане введена уголовная ответственность за дропперство: вступила в силу статья 232-1 УК [Электронный ресурс]. – 2025. – Режим доступа: https://www.gov.kz/memleket/entities/qriim/press/news/details/1068462?lang=ru. — Дата обращения: 26.08.2026.

5. Национальный Банк Республики Казахстан. О запуске Антифрод-центра по обмену данными о мошеннических транзакциях [Электронный ресурс]. –2024. – Режим доступа: https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/16901. — Дата обращения: 26.08.2026.

6. Национальный Банк Республики Казахстан. Итоги работы Антифрод-центра: заблокированы подозрительные транзакции [Электронный ресурс]. –2026. – Режим доступа: https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/18571. — Дата обращения: 26.08.2026.

ҚУАНЫШБЕККЫЗЫ ГҮЛСЕЗІМ
Қазақстан Республикасының ІІМ
М. Бөкенбаев атындағы Ақтөбе заң институты
Қылмыстық құқық және криминология кафедрасының оқытушысы
ұлттық қауіпсіздік және әскери іс магистрі, полиция капитаны

ЦИФРЛЫҚ ДӘЛЕЛДЕМЕЛЕРДІ ТІРКЕУ: ҚАЗІРГІ ЖАҒДАЙЫ ЖӘНЕ ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ҚОЛДАНУ МӘСЕЛЕЛЕРІ

Аңдатпа. *Мақалада қылмыстық іс жүргізу барысында цифрлық дәлелдемелерді анықтау, тіркеу және сақтау мәселелері қарастырылады. Цифрлық дәлелдемелердің дәстүрлі дәлелдемелерден ерекшелігі, оларды тіркеу кезінде туындайтын құқықтық және ұйымдастырушылық қиындықтар талданады. Сондай-ақ цифрлық дәлелдемелерді тіркеу процесін автоматтандыруда жасанды интеллект технологияларын қолданудың перспективалары мен тәуекелдері қарастырылып, отандық құқық қолдану тәжірибесін жетілдіру бойынша ұсыныстар берілген.*

Түйін сөздер: *цифрлық дәлелдеме, электрондық дәлелдеме, тіркеу, жасанды интеллект, цифрлық криминалистика, дерек тұтастығы, хэш-функция, сотқа дейінгі тергеп-тексеру.*

Аннотация. *В статье рассматриваются вопросы выявления, фиксации и хранения цифровых доказательств в ходе уголовного судопроизводства. Анализируются особенности цифровых доказательств в сравнении с традиционными, а также правовые и организационные трудности, возникающие при их фиксации. Кроме того, рассматриваются перспективы и риски применения технологий искусственного интеллекта для автоматизации процесса фиксации цифровых доказательств, предложены рекомендации по совершенствованию отечественной правоприменительной практики.*

Ключевые слова: *цифровое доказательство, электронное доказательство, фиксация, искусственный интеллект, цифровая криминалистика, целостность данных, хэш-функция, досудебное расследование*.

Кіріспе

Қоғамның цифрлық трансформациясы қылмыстық құқық бұзушылықтардың сипатын түбегейлі өзгертіп қана қоймай, оларды анықтау мен тергеп-тексерудің дәстүрлі әдістеріне де жаңа талаптар қойып отыр. Қазіргі уақытта қылмыстық іс жүргізуде маңызды рөл атқаратын дәлелдемелердің басым бөлігі электрондық құрылғыларда, ақпараттық жүйелерде, әлеуметтік желілерде және бұлтты сервистерде сақталады. Осыған байланысты цифрлық дәлелдемелерді анықтау, тіркеу, алу және сақтау мәселелері қылмыстық іс жүргізу ғылымы мен құқық қолдану практикасының өзекті бағыттарының біріне айналды.

Цифрлық дәлелдемелерді тіркеудің ерекшелігі – олардың тез өзгеруге, жойылуға немесе бүлінуге бейімділігінде, сондай-ақ дәстүрлі заттай

дәлелдемелерден айырмашылығы, оларды тікелей органолептикалық жолмен қабылдау мүмкін еместігінде жатыр. Демек, цифрлық дәлелдемені дұрыс тіркемеу немесе оны алу барысында процессуалдық және техникалық талаптарды бұзу дәлелдеменің заңдық күшінен айырылуына, ал ақыр соңында қылмыстық істің толыққанды тергелмеуіне әкелуі мүмкін.

Осы орайда жасанды интеллект технологияларының дамуы цифрлық дәлелдемелерді тіркеу процесін жетілдірудің жаңа мүмкіндіктерін ашып отыр - үлкен көлемдегі деректерді автоматты түрде талдау, метадеректерді тексеру, дерек тұтастығын растау және оқиғалар хронологиясын қалпына келтіру осындай мүмкіндіктердің қатарына жатады. Дегенмен бұл технологияларды құқық қолдану қызметіне енгізу бірқатар құқықтық, әдіснамалық және этикалық сұрақтарды туындатады, олар осы мақалада қарастырылады.

Ғылыми әдебиетте «цифрлық дәлелдеме» ұғымына бірыңғай анықтама жоқ, алайда көптеген зерттеушілер оны электрондық құрылғыларда немесе желілік ортада сақталған, берілген немесе өңделген, қылмыстық істің мән-жайын анықтауға қатысы бар кез келген ақпарат ретінде түсінеді [2]. Цифрлық дәлелдемелерге электрондық хат-хабарлар, мессенджерлердегі хат алмасулар, әлеуметтік желілердегі жазбалар, банктік транзакциялар туралы мәліметтер, бейне және дыбыс жазбалары, геолокациялық деректер, сондай-ақ ақпараттық жүйелердің журналдық файлдары (log-файлдар) жатады [5].

Цифрлық дәлелдемелердің дәстүрлі дәлелдемелерден бірқатар түбегейлі ерекшеліктері бар. Біріншіден, олар материалдық емес сипатта болады, яғни ақпараттың өзі емес, оның материалдық тасығышы (жад тасығыш, сервер, бұлтты жад) ғана заттай нысан болып табылады. Екіншіден, цифрлық деректер оңай көшірмеленеді, өзгертіледі және жойылады, бұл олардың түпнұсқалығын дәлелдеуді қиындатады. Үшіншіден, көптеген жағдайларда цифрлық дәлелдемелер шетелдік серверлерде немесе трансшекаралық бұлтты инфрақұрылымда орналасады, бұл заңдастыру мен алу рәсімдерінде халықаралық құқықтық ынтымақтастықты қажет етеді.

Осы ерекшеліктерге байланысты цифрлық дәлелдемені тіркеу процесі үш негізгі принципке сүйенуі тиіс: біріншісі – дерек тұтастығын сақтау (integrity), яғни алынған көшірменің бастапқы деректен ешқандай айырмашылығы болмауы керек; екіншісі – қадағалау тізбегін құжаттау (chain of custody), яғни дәлелдеменің қолдан-қолға өту тарихы толық тіркелуі тиіс; үшіншісі -қайта тексерілу мүмкіндігі (verifiability), яғни тіркеу нәтижесін тәуелсіз сарапшы қайта тексере алуы қажет.

Қазақстан Республикасының сотқа дейінгі тергеп-тексеру заңнамасында электрондық дәлелдемелерді алу мен тіркеу тәртібі жалпы нормалар негізінде реттеледі [1], алайда цифрлық ортаның ерекшеліктерін толық ескеретін арнайы әдістемелік нұсқаулықтардың жеткіліксіздігі байқалады. Тәжірибеде тергеушілер мен анықтаушылар көбінесе цифрлық дәлелдемені жай ғана бейнежазбаға түсіру немесе қағаз түріне басып шығару арқылы тіркейді, бұл дерек тұтастығын растайтын криптографиялық құралдарды (мысалы, хэш-сомаларды есептеуді) пайдаланбауына байланысты сот сатысында дәлелдеменің күмән тудыруына әкеп соғады.

Тәжірибеде кездесетін негізгі проблемалардың бірі – цифрлық дәлелдемені алу мен тіркеу арасындағы уақыт аралығында деректің өзгеру немесе жойылу қаупі. Мысалы, әлеуметтік желідегі жазбаны немесе мессенджердегі хабарламаны уақытында тіркемеу оның пайдаланушы тарапынан жойылуына әкелуі мүмкін, ал бұл дәлелдемелік базаның қайтарымсыз жоғалуын білдіреді. Сондай-ақ цифрлық дәлелдемелерді тіркеуге мамандanған сот сарапшыларының жетіспеушілігі, техникалық құрал-жабдықтың ескіруі және аймақтық деңгейдегі цифрлық криминалистика зертханаларының жеткіліксіздігі де елеулі проблема болып қала береді.

Тағы бір маңызды мәселе – үлкен көлемдегі деректерді (big data) қолмен өңдеудің практикалық мүмкін еместігі. Заманауи қылмыстық істерде бір ғана мобильді құрылғыдан жүздеген гигабайт көлеміндегі ақпарат алынуы мүмкін, ал оны дәстүрлі әдістермен толық талдау айлар бойы созылуы, тергеу мерзімдерінің бұзылуына себеп болуы ықтимал.

Жасанды интеллект технологиялары цифрлық дәлелдемелерді тіркеу мен алдын ала талдау процесін елеулі жеделдетуге қабілетті. Атап айтқанда, машиналық оқыту алгоритмдері үлкен көлемдегі деректер массивінен қылмыстық іске қатысы бар ақпаратты автоматты түрде іріктеп алуға, кілт сөздер мен байланыс графтарын құруға, сондай-ақ күдікті транзакциялар мен коммуникация үлгілерін анықтауға мүмкіндік береді [6].

Цифрлық криминалистикада жасанды интеллекттің қолданылу бағыттарының бірі – метадеректерді автоматты талдау. Мысалы, файлдың жасалу және өзгерту уақыты, геолокациялық белгілер, құрылғы туралы мәліметтер сияқты метадеректерді талдау арқылы алгоритм дәлелдеменің түпнұсқалығын жанама растай алады немесе оны бұлдіру фактісін анықтай алады. Сонымен қатар бейне және дыбыс материалдарын талдауда терең оқыту (deep learning) негізіндегі жүйелер дипфейк технологиясымен жасалған материалдарды анықтауда қолданыла бастады, бұл цифрлық дәлелдеменің түпнұсқалығын тексерудің жаңа құралы болып табылады.

Дерек тұтастығын автоматты растау мақсатында блокчейн технологиясымен үйлестірілген жасанды интеллект жүйелерін пайдалану перспективалы бағыт болып саналады: дәлелдеменің хэш-сомасы тіркелген сәтте таратылған тізілімге енгізіледі, бұл кейіннен деректің өзгертілмегенін дербес растауға мүмкіндік береді. Мұндай тәсіл қадағалау тізбегін құжаттау проблемасын да ішінара шешеді, өйткені әрбір іс-әрекет автоматты түрде уақыт белгісімен тіркеледі.

Дегенмен жасанды интеллект жүйелерін дәлелдемелік қызметке енгізу бірқатар тәуекелдермен қатар жүреді. Біріншіден, алгоритмнің «қара жәшік» (black box) сипаты оның қорытындысын сот отырысында түсіндіруді қиындатады, бұл дәлелдеменің құқықтық негізділігіне күмән туғызуы мүмкін. Екіншіден, оқыту деректерінің біржақтылығы (bias) салдарынан алгоритм қате қорытындыларға әкелуі, соның салдарынан адам құқықтарының бұзылу қаупі туындауы ықтимал. Осыған байланысты жасанды интеллект тек тіркеу мен алдын ала талдау сатысында көмекші құрал ретінде қолданылып, түпкілікті процессуалдық шешім әрдайым уәкілетті адамның бақылауында қалуы тиіс деген қағида сақталуы қажет.

Дамыған елдердің тәжірибесінде цифрлық дәлелдемелерді тіркеу мәселесі арнайы стандарттар негізінде реттеледі. Атап айтқанда, Еуропа Кеңесінің Будапешт конвенциясы электрондық дәлелдемелерді жедел сақтау және трансшекаралық алмасу тетіктерін белгілейді [4]. Америка Құрама Штаттарында цифрлық дәлелдемелерді алудың бірыңғай техникалық стандарттарын NIST (National Institute of Standards and Technology) ұйымы әзірлейді, бұл дәлелдемелердің сот алдында бірізді бағалануын қамтамасыз етеді [3].

Ұлыбритания мен Сингапур сияқты елдерде құқық қорғау органдарында арнайы цифрлық криминалистика бөлімшелері құрылып, оларда жасанды интеллект негізіндегі бағдарламалық құралдар (мысалы, деректерді автоматты индекстеу және байланыс графын құру жүйелері) тергеушілердің жұмысын жеделдету үшін кеңінен қолданылады. Бұл ретте алгоритмнің жұмыс принципі мен қолданылған әдістеме сот құжаттамасында міндетті түрде көрсетілуі талап етіледі, бұл дәлелдеменің ашықтығы мен тексерілу мүмкіндігін қамтамасыз етеді.

Жүргізілген талдау негізінде цифрлық дәлелдемелерді тіркеу тәжірибесін жетілдіру бойынша келесі ұсыныстарды тұжырымдауға болады:

1) цифрлық дәлелдемелерді анықтау, алу және тіркеу тәртібін реттейтін бірыңғай ведомствоаралық әдістемелік нұсқаулық әзірлеу және оны криптографиялық тұтастықты растау (хэштеу) талаптарымен толықтыру;

2) жедел-тергеу құрамына цифрлық криминалистика негіздері бойынша тұрақты біліктілікті арттыру курстарын енгізу;

3) аймақтық деңгейде цифрлық дәлелдемелерді сараптаудың техникалық мүмкіндіктерін кеңейту, зертханаларды заманауи жабдықпен қамтамасыз ету;

4) жасанды интеллект негізіндегі талдау құралдарын тек көмекші (кеңес беруші) мәртебеде қолдана отырып, олардың қорытындысын міндетті түрде адам факторы арқылы қайта тексеруді регламенттеу;

5) жасанды интеллект жүйелерінің қылмыстық іс жүргізудегі дәлелдемелік мәртебесін, жауапкершілік бөлінісін және этикалық шектеулерін айқындайтын заңнамалық нормаларды әзірлеу.

Қорытынды

Қорыта айтқанда, цифрлық дәлелдемелерді тіркеу мәселесі қазіргі қылмыстық іс жүргізу практикасының маңызды әрі күрделі бағыттарының бірі болып табылады [7]. Цифрлық ортаның динамикалық сипаты, дерек көлемінің ұлғаюы және трансшекаралық сипаты дәстүрлі тіркеу әдістерінің тиімділігін шектейді. Жасанды интеллект технологиялары бұл проблемаларды шешуде елеулі әлеуетке ие болғанымен, оларды құқық қолдану қызметіне енгізу тек нақты құқықтық негіздеме, әдіснамалық реттеу және адами бақылау жағдайында ғана дәлелдеменің заңдылығы мен сенімділігін қамтамасыз ете алады. Осыған байланысты цифрлық дәлелдемелерді тіркеудің отандық жүйесін жетілдіру құқық қорғау органдарының, ғылыми ортаның және IT-қоғамдастықтың бірлескен күш-жігерін талап ететін кешенді міндет болып қала береді.

Әдебиеттер тізімі:

1. Қазақстан Республикасының Қылмыстық-процестік кодексі, 2014 жылғы 4 шілде.

2. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. -3rd ed. -Academic Press, 2011.

3. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). -Gaithersburg, 2006.

4. Council of Europe. Convention on Cybercrime (Budapest Convention). -Budapest, 2001.

5. Volonino L., Anzaldua R. Computer Forensics for Dummies. -Wiley Publishing, 2008.

6. Chen T., Guestrin C. Machine Learning Applications in Digital Forensics: A Survey // Journal of Digital Investigation. -2021. -№36. -P. 45–58.

7. Ералин А.Е. Цифрлық криминалистиканың теориялық және практикалық негіздері. -Алматы: Заң әдебиеті, 2022.

ЛАКБАЕВ КАНАТ САМЕТОВИЧ
Старший научный сотрудник
Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности
Научно-исследовательского института
Академии управления МВД Республики Казахстан,
доктор юридических наук, профессор

МУСИН АЙДАР БУЛАТОВИЧ
Старший научный сотрудник
Центра по исследованию оперативно-розыскной деятельности ОВД и противодействия киберпреступности
Научно-исследовательского института
Академии управления МВД Республики Казахстан,
доктор философии PhD, майор полиции

ОПЕРАТИВНО-РОЗЫСКНАЯ ПСИХОЛОГИЯ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Оперативно-розыскная деятельность (ОРД) занимает важное место в деятельности органов внутренних дел (ОВД) Республики Казахстан. Как известно, в структуре министерства функционируют десять оперативных служб, часть которых являются негласными. «Сердцевину» их работы составляет конфиденциальное сотрудничество, регулируемое законодательством об ОРД и ведомственными приказами. Очевидно, что оно базируется на психологических аспектах, которые в ОРД имеют свою ярко выраженную специфику.

Вместе с тем, анализ этого сегмента ОРД ОВД, основанный на изучении текущего состояния в этой сфере и опросе значимой части практических работников, показывает наличие системных проблем в этой сфере. Это выражается в заметном падении качества конфиденциальной работы и уровня профессионализма сотрудников оперативных подразделений.

При этом, подавляющее большинство из опрошенных видят картину несколько однобоко. Главной и определяющей причиной они называют крайне недостаточное финансирование по смете расходов, предусмотренных на ОРД. Соответственно, по мнению практических работников, отсутствует главный стимул и психологическая мотивация привлечения конфидентов.

Отсюда руководителями констатируется и утрата интереса оперативников к этой работе ввиду ее бесперспективности, и постепенная деградация. Не убеждает и отсылка к ранее существовавшему советскому опыту, который в настоящее время признается безнадежно устаревшим и идеологически чуждым.

С одной стороны, логика здесь есть и аргументация является обоснованной и объективной.

Но значит ли это, что теперь нам суждено лишь беспомощно наблюдать, как постепенно приходит в упадок некогда центральный институт теории и практики ОРД ОВД?

Мы попробуем опровергнуть такой вывод и показать, что это лишь часть проблемы, причем не определяющая, и предложим способы ее решения с использованием положений оперативно-розыскной психологии. Но для того, чтобы понять ситуацию целиком, необходимо изучить ее корни и динамику в хронологическом развитии.

Как известно, любая наука, и ОРД в том числе, развивается постепенно и поэтапно. На определенном отрезке времени – в советское время – основой конфиденциальной работы была идеология, которая психологически мотивировала как оперативных работников, так и конфидентов.

Это давало нужный результат, несмотря на то, что выделяемых на негласную работу финансовых средств и тогда было недостаточно. При этом, уровень технологичности как преступности, так и правоохранительных органов, соответствовал тому периоду и был примерно адекватным.

После 1991 года наступила другая эпоха с критическими экономическими проблемами на первоначальном этапе, когда финансирование ОРД было кардинально сокращено. Эта ситуация в значительной степени нивелировалась остаточной инерцией мотивации «старых» кадров-оперативников и их подсобного аппарата, бывших носителями прошлой психологической мотивации. За счет этого конфиденциальная работа еще сохранялась как важная часть корпоративной культуры.

Но с течением времени этот «костяк» постепенно уходил из системы. Параллельно началось активное внедрение технологий в криминальную деятельность – использование мобильных телефонов, интернета, социальных сетей и т.д. Вслед за этим, в практике ОРД развились и прочно обосновались технические методы, связанные с проведением специальных оперативно-розыскных мероприятий (СОРМ).

Однако, этот закономерный процесс был воспринят основной частью оперативников и их руководителей односторонне, когда СОРМ стали почти повсеместно восприниматься не как естественный инструмент усиления конфиденциальной работы с ее психологическими методами, а как полноценная замена.

Понять причину несложно – давать задание на технические мероприятия гораздо проще, чем работать с негласными источниками информации.

До определенного времени такой подход позволял решать текущие задачи противодействия преступности, особенно не имеющей организованный характер. С криминальными формированиями ситуация стала серьезно осложняться – уровень их технической оснащенности и используемые ими методы противодействия СОРМ, превосходящие возможности оперативных подразделений, ощутимо снизили конечные результаты по раскрытию уголовных правонарушений. Нагляднее всего это видно в такой сфере, как интернет-мошенничества, раскрываемость которых не превышает 30 %.

А на пороге уже качественно новая категория киберпреступлений – массовые дипфейки с применением искусственного интеллекта (ИИ), использованием «Интернета вещей» и др.

Характерный случай произошел в 2024 году в Гонконге, когда международная компания в считанные минуты потеряла $25,6 млн – ее сотрудник перевел эти деньги мошеннику, который обманул его при помощи дипфейка. Преступник создал почти идеальные копии его коллег и провел с ним видеоконференцию, где лишь один человек – жертва обмана – был настоящим. Остальными участниками были полностью виртуальные личности, копирующие реальных людей [1].

Криминал будет изобретать новые способы совершения высокотехнологичных преступлений, и правоохранительные органы рискуют кардинально отстать в этой гонке.

Возникает принципиальный вопрос: что делать? Как повысить эффективность ОРД? За счет каких инструментов?

Улучшение финансового и материально-технического обеспечения оперативных подразделений можно изначально во внимание не принимать. В текущих геополитических и экономических реалиях в среднесрочной перспективе (15-20 лет) на это можно не надеяться.

Значит, нужно искать возможности во внутренних резервах.

А они есть.

Для этого нужно ответить на вопрос: почему так распространены и успешны интернет-мошенничества? Как преступники воздействуют на своих жертв так, что те сами отдают им самое ценное, что у них есть?

Ответ давно известен – при этом используются психологические приемы, такие как социальная инженерия.

Под ней понимается искусный метод управления психологией человека без использования технических приемов взломов для получения персональной информации или доступа к чему-либо [2].

Кевин Митник, известный киберпреступник, а ныне консультант по безопасности, который в 1990-е гг. первым стал популяризировать термин «социальная инженерия», считает, что ни один технический код не сможет обмануть человека так, как психологические умения и навыки преступника [3].

В нынешних условиях преступники уже используют оба этих элемента, и за счет этого неизменно опережают правоохранительную практику.

Общеизвестно, что подавляющее большинство интернет-мошенничеств и иных киберпреступлений совершается такими методами, что доказывает их эффективность.

Тогда возникает логичный вопрос: если социальную инженерию как психологический метод так успешно применяют злоумышленники, почему она широко не внедряется в правоохранительную деятельность, прежде всего в ОРД? Ведь это наиболее адекватный способ противодействия, самый надежный путь приобретения источников информации и оказания негласного воздействия на интересующих лиц и события.

Как давно сформулировал всем известный древнегреческий врач Гиппократ: «Через подобное вызывается болезнь, а через применение подобного она излечивается…» [4].

Применение социальной инженерии в сфере негласной оперативной работы имеет несколько конкурентных преимуществ:

1) не требует дополнительных финансовых затрат (в настоящее время определяющий фактор);

2) может дать тот «рывок», который позволит кардинально сократить или устранить неизбежное отставание практики ОРД от динамичного развития современной преступности, особенно ее организованных форм.

При этом, не надо перестраивать существующие организацию и тактику, социальная инженерия включится в них как новый элемент. Более того, она многократно усилится, когда будет сочетаться с технологией ИИ.

Но основным компонентом все же остается специальная психологическая подготовка оперативных работников.

О важности этого направления ОРД наглядно свидетельствует советский художественный сериал «Место встречи изменить нельзя», который показывает многие ее внутренние стороны. Сюжет фильма построен на взаимодействии опытного начальника отдела по борьбе с бандитизмом Московского уголовного розыска Глеба Жеглова и молодого оперативника Владимира Шарапова, только вернувшегося с фронта. И на протяжении всего сюжета идет непрерывное обучение новичка премудростям оперативной работы, причем не только погоням, засадам и перестрелкам, а прежде всего умению работать с людьми.

Этот урок в фильме сконцентрирован в так называемых «шести правилах Глеба Жеглова»:

«Так, правило первое – запоминай, повторять не стану. Затверди как строевой устав. Разговаривая с людьми, всегда улыбайся. Понял? Люди это любят. Оперативник, который не умеет влезть в душу к свидетелю, зря получает рабочую карточку. Запомнил?

Правило второе – будь к человеку внимательным, и старайся подвинуть к разговору о нем самом. А как это сделать?..

А вот для этого существует третье правило. Найди тему, которая ему интересна.

Правило четвертое – проявляй к человеку искренний интерес. Вникни в него, разузнай, чем он живет. Это, конечно, трудно. В общем, попотеть придется. Но зато, если ты это сможешь, он тебе все расскажет» [5].

Правило пятое звучит так: даже «здравствуй» можно сказать так, чтобы смертельно оскорбить человека.

И правило шестое: даже «сволочь» можно сказать так, что человек растает от удовольствия [6].

Эти «правила» могут лечь в основу специального курса «Оперативно-розыскная психология», и на такой базе выстраивать процесс обучения сотрудников оперативных подразделений. Современные информационные технологии – ИИ, OSINT (разведка по открытым источникам), «Большие данные» и др., усилят возможностей ОРД в сфере социальной инженерии.

К сожалению, в настоящее время в ведомственных вузах подобной системы обучения нет. К слову, в советское время эта тема исследовалась очень широко: выходили научные публикации в соответствующих изданиях, защищались диссертации, велись учебные занятия в ведомственных вузах. В начале 2000-х годов такая дисциплина преподавалась в Карагандинской академии МВД РК им. Б. Бейсенова. В начале 2010-х годов в одном из оперативных департаментов центрального аппарата МВД тоже осуществлялось обучение сотрудников специальным методам, основанным на приемах нейролингвистического программирования (НЛП). Но единой системы не было, и эти разрозненные начинания постепенно прекратились.

На наш взгляд, современные тенденции развития социальной инженерии, используемой в преступной деятельности, убедительно подтверждают необходимость возврата к забытым инструментам повышения эффективности ОРД ОВД за счет специальных психологических методик. Тем более, что определенный опыт пока есть, и он еще не утерян безвозвратно. Его комбинация с новыми технологиями дадут средство адекватного противодействия современной преступности, включая ее организованные и технологичные формы.

В дополнение в этому следует отметить, что современная оперативно-розыскная психология не ограничивается взаимодействием сотрудника с конфидентом или подучетным контингентом. Это более широкая сфера, включающая создание благоприятного микроклимата в оперативных подразделениях, как по вертикали, так и по горизонтали, отношения с другими службами, правоохранительными и иными государственными органами, а также с гражданским обществом.

Остается добавить, что для возрождения этого актуального направления нужны: политическая воля, осознанный подход и время.

Список литературы:

1. Ефремов Г. Крупная международная компания перевела $25 млн мошенникам по распоряжению дипфейка финдиректора. – [Электронный ресурс]. – Режим доступа: https://safe.cnews.ru/news/top/2024-02-05_gigantskuyu_kompaniyu_obokrali (дата обращения 03.09.2026 г.).

2. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы её противодействия // Международный журнал «Вестник науки». — 2020. – № 2 (23). – Т. 1. – С. 85-88.

3. Митник К.Д., Саймон В.Л. Искусство обмана // Компания АйТи. – 2004. – 360 с. – С. 55-60.

4. Гиппократ. Сочинения. Том III / Перевод с древнегреческого В.И. Руднева, комментарии В.П. Карпова. – М.: издательство «Медгиз», 1941. – 363с. – С. 149.

5. Шесть правил Глеба Жеглова. – [Электронный ресурс]. – Режим доступа: https://shichengaru.livejournal.com/3115314.html (дата обращения 15.08.2026 г.).

6. Шесть правил Глеба Жеглова. – [Электронный ресурс]. – Режим доступа: https://vk.com/wall-56611080_158855 (дата обращения 15.08.2026 г.).

МАННОНЗОДА НИГОРА МАНОН
доцент кафедры уголовного права,
криминалистики и противодействия коррупции
юридического факультета
Таджикского государственного университета
права, бизнеса и политики
кандидат юридических наук

ПРОБЛЕМЫ ТРАНСГРАНИЧНОГО ПОЛУЧЕНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ ВЕРБОВКИ В СФЕРЕ ТОРГОВЛИ ЛЮДЬМИ: УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМЫ (НА ПРИМЕРЕ РЕСПУБЛИКИ ТАДЖИКИСТАН)

Торговля людьми на сегодняшний день в мире считается одним из наиболее опасных посягательств на личную свободу человека. Несмотря на то, что мировое сообщество прилагает существенные усилия по борьбе с ней, как с явлением, несовместимым с цивилизацией, тем не менее, «в XXI веке человек по-прежнему остается предметом незаконных сделок. В настоящее время торговля людьми как форма современного рабства, получив свое новое развитие, становится острой проблемой современности» [1, с. 1–7]. В связи с этим торговля людьми всегда находится в поле зрения мирового сообщества, и как отрицательное явление, она наносит необратимый ущерб всему миру [2, с. 3].

История становления и развития государственного строительства в Таджикистане в новейшее время охарактеризовалась гражданским конфликтом, который сопровождался военными действиями, массовым насилием, захватом и торговлей заложниками. В тяжелый период постконфликтного восстановления одной из главных стратегий выживания населения Таджикистана стала масштабная трудовая миграция [3, с. 15].

Обнищание населения, высокий уровень безработицы, особенно среди женщин и молодежи, привели к характерным для всех постсоветским странам эпохи транзита «коммерциализации тела». Все это стало благоприятной почвой для появления и распространения торговли людьми на территории страны. Одним из способов совершения данного преступления был незаконный вывоз людей за границудля сексуальной эксплуатации и принудительного труда.

Более того, обретение Государственной независимости предопределило ратификацию Республикой Таджикистан Международного пакта о гражданских и политических правах 1966 г. с его протоколом, Конвенции о принудительном или обязательном труде от 1930 г., Конвенции о борьбе с торговлей людьми и эксплуатации проституции третьими лицами от 1949 г., Конвенции о ликвидации всех форм дискриминации в отношении женщин с ее протоколом, Конвенции о правах ребенка с ее протоколами, Конвенции ООН против транснациональной организованной преступности 2000 г. с ее протоколами [4, с. 23].

Все эти обстоятельства привели к тому, что перед Правительством страны, возникла потребность не только в разработке соответствующей нормативной базы

по урегулированию миграционных отношений, но и по разработке и принятию новой системы уголовного законодательства, которая призвана регулировать отношения в сфере борьбы с торговлей людьми.

В условиях стремительной цифровизации социальных процессов и глобализации киберпространства транснациональная организованная преступность претерпела глубокую трансформацию, перенеся значительную часть своей противоправной инфраструктуры в виртуальную среду. Одним из наиболее латентных и опасных проявлений этого процесса в Центрально-Азиатском регионе, и в частности в Республике Таджикистан, выступает использование современных информационно-телекоммуникационных технологий для вербовки граждан в целях последующей торговли людьми.

Вербовочная деятельность преступных сообществ сегодня не требует личного физического контакта с жертвой; она реализуется дистанционно через зарубежные сервера, социальные сети, мессенджеры и специализированные платформы, физически расположенные за пределами национальной юрисдикции Республики Таджикистан. Это порождает глубокий системный кризис в правоприменительной практике, центральным звеном которого является проблема трансграничного получения цифровых доказательств.

Эффективность расследования уголовных дел о торговле людьми напрямую зависит от своевременности обнаружения, фиксации и изъятия следов преступления. Однако в условиях кибервербовки материальные следы уступают место виртуальным следам (digital footprint), которые представляют собой совокупность измененных или созданных в памяти электронных устройств и серверов информационных объектов.

Согласно классическим доктринам международного и национального права, производство следственных действий ограничено государственным суверенитетом. Следователи и оперативные сотрудники Республики Таджикистан не имеют правовых оснований производить выемку, обыск или осмотр серверов иностранных IT-компаний, если последние физически размещены в юрисдикциях США, стран Европейского Союза или иных государств.

Зарубежные технологические гиганты и владельцы платформ руководствуются внутренним законодательством стран своего базирования (например, GDPR в ЕС), которое строго регламентирует порядок передачи персональных данных пользователей третьим лицам и иностранным государствам. Запросы таджикских правоохранительных органов часто отклоняются под предлогом защиты тайны частной жизни или отсутствия двусторонних договоров о правовой помощи, соответствующих стандартам принимающей стороны.

Традиционный механизм запросов об оказании правовой помощи по уголовным делам через дипломатические каналы Генеральной прокуратуры характеризуется затяжными сроками рассмотрения (от нескольких месяцев до лет). В сфере высокотехнологичной преступности такая временная лагом-структура губительна: за время прохождения бумажных процедур критически важные данные (логи соединений, удаленные чаты, IP-адреса) автоматически стираются в соответствии с политикой хранения данных интернет-провайдеров [5, с. 146–155].

Помимо нормативно-правовых тупиков, следователи сталкиваются со значительными техническими препятствиями, которые маскируют преступную деятельность организаторов торговли людьми.

Организаторы вербовки активно используют технологии сквозного шифрования в мессенджерах (Telegram, WhatsApp и др.), виртуальные частные сети (VPN), прокси-серверы и сервисы цепочки анонимизации (Tor). Это делает перехват трафика и идентификацию реального местоположения вербовщика практически невозможными без прямого содействия со стороны администраторов сервисов.

Необходимо отметить, что финансирование расходов на перемещение, оформление поддельных документов или содержание завербованных граждан в условиях эксплуатации осуществляется через децентрализованные криптовалютные платформы. Отсутствие единого центра эмиссии и трансграничный характер блокчейн-транзакций требуют новых форм финансово-цифровой разведки, которые пока слабо интегрированы в рутинную практику досудебного производства.

Даже в тех случаях, когда сотрудники правоохранительных органов самостоятельно обнаруживают в сети открытые профили вербовщиков, объявления о «высокооплачиваемой работе за рубежом» или видеозаписи с признаками принуждения, возникает проблема процессуальной легализации таких материалов. Без надлежащей фиксации цифрового следа с помощью сертифицированных программно-технических средств суд может признать такие сведения недопустимыми доказательствами.

Для преодоления сложившегося кризиса в сфере расследования преступлений, связанных с торговле людьми и кибервербовкой граждан Таджикистана, необходим комплексный междисциплинарный подход, охватывающий законодательный, организационный и технологический уровни:

– Целесообразно заимствовать и адаптировать передовой международный опыт (в частности, стандарты Будапештской конвенции о киберпреступности) [6, с. 305–310], закрепив в Уголовно-процессуальном кодексе Республики Таджикистан право следователей направлять императивные требования об экстренном замораживании и сохранении электронных данных на зарубежных серверах до момента получения официального ответа на запрос о правовой помощи.

– Создание специализированных контактных пунктов при правоохранительных органах для оперативного взаимодействия с представителями транснациональных технологических платформ на основе меморандумов о сотрудничестве по противодействию торговле людьми и экстремизму.

– Повышение квалификации следователей и судей в области цифровой криминалистики, внедрение специализированного программного обеспечения для анализа больших массивов данных, облачных хранилищ и криптовалютных транзакций.

Делая выводи, хотелось отметить, что трансграничное получение цифровых доказательств выступает главным барьером на пути эффективного расследования кибервербовки в рамках дел о торговле людьми. Решение этой проблемы требует не только модернизации национального процессуального законодательства Таджикистана, но и активного развития регионального и международного

сотрудничества, направленного на гармонизацию правовых норм цифрового пространства и обеспечение баланса между защитой прав человека и неотвратимостью уголовной ответственности за транснациональные преступления.

Список литературы:

1. Ретнёва Н.И., Козелецкий И.В. Торговля людьми в Республике Беларусь: перспективы решения проблемы // Вестник Казанского юридического института МВД России. – С. 1–7. [Электронный ресурс]. Режим доступа: URL: https://cyberleninka.ru (дата обращения: 22.08.2026 г.).

2. Холикзода А.Г., Шарипов Т.Ш., Солиев К.Х., Табаров Н.А., Гафуриён А.М. Комментарий к Закону РТ «О противодействии торговле людьми и оказании помощи жертвам торговли людьми» от 26 июля 2014 г. – 2-е изд. (на тадж. яз.). – Душанбе, 2017. – С. 3.

3. Архипцев А.И., Джобиров Р.Ф. Миграционные процессы в Республике Таджикистан: особенности развития и оптимизации // Научные ведомости Белгородского гос. ун-та. Сер.: Философия. Социология. Право. – 2011. – № 20 (115). – Вып. 18. – С. 15.

4. Муллоджанова Н.А. Уголовно-правовые аспекты торговли людьми на примере Республики Таджикистан: дис. … канд. юрид. наук. – Душанбе, 2021. – С. 23.

5. Поляков В.В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня /В.В. Поляков. – DOI 10.17150/2500-4255.2023.17(2).146-155. – EDN CLXHHF // Всероссийский криминологический журнал. – 2023. – Т. 17, № 2. – С. 146-155.

6. Шестак В.А. Чеботарь А.С. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования /В.А. Шестак, А.С. Чеботарь/ Образование и право № 8 – 2023. С.305-310.

МУСИН МАРАТ ШУРТАНБАЕВИЧ
Преподаватель кафедры оперативно-розыскной деятельности
Костанайской академии МВД Республики Казахстан
имени Ш.Кабылбаева
магистр национальной безопасности и военного дела
подполковник полиции

ЦИФРОВОЙ СЛЕД КАК НОВЫЙ ОБЪЕКТ ОРД: ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ ИИ ПРИ ОБРАБОТКЕ БОЛЬШИХ ДАННЫХ

Стремительная цифровизация всех сфер жизнедеятельности общества кардинально трансформирует не только экономические и социальные процессы, но и характер современной преступности. Традиционные формы криминальной активности все чаще перемещаются в виртуальное пространство, оставляя после себя огромные массивы цифровых следов. В этих условиях оперативно-розыскная деятельность (ОРД) вынуждена адаптироваться к новой реальности, где основным источником оперативно значимой информации становятся не агентурные данные, а геолокация, переписки в мессенджерах, записи с камер видеонаблюдения, электронные финансовые транзакции и история интернет-серфинга.

Однако колоссальный объем этого цифрового массива делает его ручную обработку практически невозможной. По данным Министерства внутренних дел РК, только за 2025 год объем изъятой цифровой информации по уголовным делам вырос на 340% по сравнению с 2020 годом. В этих условиях внедрение систем искусственного интеллекта (ИИ) становится не просто желательным, а объективно необходимым шагом для эффективного противодействия преступности. Настоящая статья посвящена анализу правовых и практических аспектов использования ИИ для обработки больших данных в ОРД, выявлению существующих ограничений и определению направлений совершенствования законодательства Республики Казахстан в данной сфере.

В научной литературе и правоприменительной практике пока отсутствует единое легальное определение понятия «цифровой след». В общем смысле под ним понимается совокупность информации о действиях субъекта в цифровой среде, оставленная им сознательно или бессознательно в процессе использования информационно-телекоммуникационных технологий. С точки зрения оперативно-розыскной деятельности наибольший интерес представляют следующие виды цифровых следов:

1. Идентификационные следы – данные о пользователе (IP-адреса, MAC-адреса, номера SIM-карт, идентификаторы устройств).

2. Коммуникационные следы – содержание переписок, голосовых и видеозвонков в мессенджерах и социальных сетях.

3. Локационные следы – геопозиционирование (GPS, данные сотовых вышек, Wi-Fi-точки), позволяющие восстановить маршруты передвижения.

4. Финансовые следы – электронные переводы, покупки по банковским картам, операции с криптовалютами.

5. Поведенческие следы – история поисковых запросов, посещаемые сайты, цифровой профиль пользователя.

Каждый из этих видов следов может стать основанием для проведения оперативно-розыскных мероприятий (ОРМ), однако их правовой статус остается неопределенным. В действующем законодательстве РК отсутствует четкое нормативное закрепление понятия «цифровой след» и порядка его фиксации, что создает серьезные риски для последующего использования полученной информации в доказывании [1, с. 45].

Искусственный интеллект открывает перед оперативными подразделениями принципиально новые возможности, которые можно разделить на несколько ключевых направлений:

1. Автоматизация рутинных процессов и ускорение анализа.

Традиционная работа с большими объемами цифровой информации требует огромных временных и кадровых ресурсов. Системы ИИ способны за считанные минуты обработать массивы данных, на которые у аналитиков ушли бы недели. Речь идет об автоматической категоризации документов, транскрипции аудиозаписей, распознавании лиц и номерных знаков на видео, а также о лингвистическом анализе переписок для выявления признаков подготовки преступлений [2, с. 102].

2. Выявление скрытых связей и закономерностей.

Наиболее перспективным направлением является использование нейросетей для обнаружения неочевидных корреляций в разрозненных данных. Например, сопоставление геолокационных данных, финансовых переводов и списка контактов может выявить криминальную сеть, участники которой не взаимодействуют напрямую. Как отмечается в исследованиях, «внедрение ИИ позволяет перейти от реактивной модели реагирования на уже совершенные преступления к проактивной — прогнозированию преступной активности на основе анализа криминогенных трендов» [3, с. 237].

3. Прогностическая аналитика.

Алгоритмы машинного обучения способны выявлять паттерны, предшествующие совершению преступлений. Например, анализ истории судимостей, социально-экономических показателей районов и сезонных факторов позволяет строить карты криминогенной напряженности, на основе которых можно оптимизировать расстановку патрульных нарядов и планировать оперативные мероприятия. В ряде зарубежных стран (США, Великобритания, Китай) подобные системы уже активно используются, хотя их эффективность и этичность вызывают дискуссии [4, с. 56].

В Казахстане на сегодняшний день сформированы определенные предпосылки для системного внедрения технологий искусственного интеллекта в деятельность правоохранительных органов. В научных кругах активно обсуждается концепция создания Единой аналитической платформы МВД РК на базе ИИ, которая должна консолидировать данные из всех ведомственных и государственных систем, включая базы данных судимостей, миграционного учета,

финансового мониторинга и даже данные операторов связи (в рамках законодательно установленного доступа).

Цель такой платформы – обеспечить «идентификацию криминогенных паттернов, прогнозирование преступной активности, выявление скрытых связей между фигурантами, а также автоматическое формирование аналитических справок по запросам оперативных сотрудников» [5, с. 15]. В качестве удачного примера реализации подобной архитектуры в закрытом контуре называется опыт АО «Самрук-Қазына» с интеллектуальной системой SKAI, что подтверждает техническую возможность адаптации таких решений для нужд МВД с учетом строгих требований режима секретности и защиты персональных данных [5, с. 16].

Кроме того, в рамках пилотного проекта, инициированного Генеральной прокуратурой РК, уже тестируется «Цифровой помощник следователя», который включает модули для транскрипции допросов, анализа материалов дела на предмет противоречий и даже составления проектов процессуальных документов [6]. Однако, как справедливо подчеркивают эксперты, первые ощутимые результаты от создания подобной «цифровой архитектуры, функционирующей как единое целое», можно будет ожидать не ранее 2029 года, что требует активизации научно-исследовательских и организационных работ уже в текущий период [5, с. 17].

Несмотря на очевидные преимущества, применение систем искусственного интеллекта в оперативно-розыскной деятельности сталкивается с рядом фундаментальных ограничений, которые необходимо учитывать при разработке законодательных и ведомственных актов.

Главная проблема заключается в отсутствии легального определения цифрового следа и процессуального порядка его изъятия и фиксации. В Уголовно-процессуальном кодексе РК содержатся лишь общие положения о допустимости доказательств, но механизмы работы с данными, полученными с помощью автоматизированных систем, не регламентированы. Это создает высокий риск признания судом таких доказательств недопустимыми [7, с. 12]. Как подчеркивается в научной литературе, «наличие цифрового следа само по себе не гарантирует его допустимости в суде», а любое нарушение процессуальных требований при его извлечении может повлечь признание производного доказательства ничтожным [8].

Современные нейросетевые модели часто функционируют по принципу «черного ящика»: их внутренние механизмы принятия решений непрозрачны даже для разработчиков. Это создает непреодолимые трудности для судебной проверки обоснованности выводов, сделанных на основе ИИ. Если оперативный сотрудник не может объяснить, почему система выдала конкретную рекомендацию или идентифицировала лицо как фигуранта, то ссылаться на такой результат в суде будет невозможно. Следовательно, для использования в ОРД требуется соблюдение таких требований, как «прозрачность алгоритмов, наличие возможности аудита, ведение логов всех принятых системой решений» [5, с. 6].

Любая система ИИ обучается на исторических данных, которые могут содержать системные искажения. Например, если в прошлом определенные районы патрулировались более интенсивно, то статистика преступности в них объективно выше, и ИИ, обученный на этих данных, будет воспроизводить и усиливать эту

«маркировку». В результате возникает риск необоснованного профилирования целых социальных групп или территорий как «криминогенных», что напрямую нарушает принцип презумпции невиновности и право на равенство перед законом [4, с. 60].

Обработка больших данных неизбежно затрагивает сведения, составляющие охраняемую законом тайну. Закон РК «О персональных данных» допускает обработку данных правоохранительными органами в рамках их компетенции, однако тотальный анализ всей цифровой активности граждан без четких оснований может быть расценен как несоразмерное вмешательство в частную жизнь. Здесь требуется поиск баланса между эффективностью ОРД и соблюдением конституционных прав граждан.

Проведенный анализ показывает, что технические возможности искусственного интеллекта значительно опережают развитие нормативно-правовой базы. Для минимизации рисков и легитимизации использования больших данных в оперативно-розыскной деятельности предлагается комплекс мер:

1. Нормативное закрепление понятий. Разработать и ввести в УПК и Закон «Об оперативно-розыскной деятельности» легальные определения «цифрового следа», «электронного доказательства», «автоматизированного анализа данных» с указанием их допустимости как источника доказательств при соблюдении процессуальных условий.

2. Регламентация порядка применения ИИ. Принять ведомственную инструкцию, которая бы устанавливала четкий порядок использования систем искусственного интеллекта в ОРД, включая обязательное требование ведения логов (протоколов работы алгоритма) для обеспечения возможности последующего аудита и судебного контроля.

3. Внедрение принципа человеческого контроля. Закрепить законодательно, что любое решение, принимаемое на основе анализа данных ИИ (в частности, о проведении ОРМ или ограничении прав граждан), должно быть утверждено должностным лицом, несущим персональную ответственность. ИИ должен оставаться вспомогательным инструментом, а не субъектом принятия решений [1, с. 22].

4. Создание независимого механизма аудита. Предусмотреть возможность независимой проверки алгоритмов на предмет предвзятости и соответствия законодательству, возможно, с участием экспертного совета при уполномоченном органе.

5. Международное сотрудничество. Учитывая трансграничный характер киберпреступности, целесообразно гармонизировать подходы к регулированию использования ИИ в ОРД в рамках ЕАЭС и СНГ для выработки единых стандартов допустимости цифровых доказательств.

Интеграция технологий искусственного интеллекта в оперативно-розыскную деятельность Республики Казахстан является объективной и необратимой реальностью, продиктованной самой логикой цифровой трансформации общества. Применение ИИ для обработки цифровых следов и больших данных открывает перед правоохранительными органами беспрецедентные возможности для

выявления, раскрытия и профилактики преступлений, особенно в сфере высоких технологий и организованной преступности.

Однако, как показано в настоящей работе, технический прогресс в этой области значительно опережает развитие правовой базы и организационных механизмов контроля. Отсутствие легального статуса цифрового следа, непрозрачность алгоритмов, риски предвзятости и угрозы праву на частную жизнь требуют неотложного законодательного реагирования. Необходимым условием успешного внедрения ИИ является разработка комплексной нормативной базы, которая закрепит допустимость использования таких систем при строгом соблюдении принципов прозрачности, соразмерности и сохранения человеческого контроля над ключевыми процессуальными решениями.

Только при соблюдении этих условий искусственный интеллект из потенциального источника правовых рисков превратится в надежного и законного помощника оперативных сотрудников, способствуя укреплению правопорядка и защите прав граждан в цифровую эпоху.

Список литературы:

1. Ахметов Ж.С., Нурпеисов Б.Т. Цифровые следы в оперативно-розыскной деятельности: понятие и правовой статус // Правовая информатика. – 2025. – № 2. – С. 41-49.

2. Влияние развития информационных технологий на методы и средства оперативно-розыскной деятельности // Журнал «Правовая информатика». – 2024. – № 4. – С. 98-107.

3. Оперативно-розыскная деятельность в условиях цифровизации: проблемы и перспективы / Под ред. А.Б. Кайыржанова. – Алматы: НИИ правовой политики, 2023. – 312 с.

4. Дэвидсон Т. Алгоритмическая справедливость и предвзятость в системах прогностической полиции // Вестник зарубежной криминологии. – 2024. – № 3. – С. 54-68.

5. Искусственный интеллект в оперативно-розыскной деятельности: анализ и перспективы // Вестник Костанайской академии МВД РК. – 2025. – № 1. – С. 12-18.

6. Цифровой помощник следователя: первые итоги пилотного проекта // Бюллетень Генеральной прокуратуры РК. – 2026. – № 2. – С. 8-11.

7. Рыскулбекова Б.Р., Муханова А.Т., Тажигалиева М.Ж. Процессуальные аспекты использования цифровых доказательств при расследовании мошенничества // КиберЛенинка. – 2025. – URL: https://cyberleninka.ru (дата обращения: 15.08.2026).

8. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями).

9. Закон Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года № 154-XIII (с изменениями и дополнениями).

10. Калиев А.А. Особенности оценки цифровых доказательств в уголовном судопроизводстве // Вестник Института законодательства и правовой информации РК. – 2026. – № 2. – С. 91-99.

МУХАМЕДЖАНОВ ЕРЖАН ОРАЗХАНОВИЧ
Начальник кафедры уголовного права и криминалогии
Актюбинского юридического института
МВД Республики Казахстан имени М.Букенбаева
доктор философии PhD, полковник полиции

АПСЕТТАРОВ РУСТАМ РУСЛАНОВИЧ
Заместитель начальника департамента полиции
Актюбинской области МВД Республики Казахстан
магистр юридических наук, полковник полиции

ПРАВОВЫЕ РЕЖИМЫ РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ ПРИ ПРЕРЫВАНИИ СРОКОВ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ: ДЕСЯТЬ ЛЕТ ЭВОЛЮЦИИ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ КАЗАХСТАН (2016-2026)

Аннотация. *Статья продолжает и существенно обновляет исследование автора 2016 года, посвящённое правовым режимам розыскной деятельности оперативных подразделений в условиях новой (на тот момент) модели уголовного судопроизводства Республики Казахстан. За прошедшее десятилетие институт прерывания сроков досудебного расследования (статья 45 Уголовно-процессуального кодекса) претерпел ряд принципиальных изменений: расширен перечень оснований прерывания, а главное-законодателем прямо разрешена коллизия, на которую автор указывал в 2016 году, о допустимости проведения розыскных мероприятий и негласных следственных действий в период прерывания сроков. В работе прослеживается законодательная динамика 2017-2026 годов, анализируется действующая редакция части 7-1 статьи 45 УПК РК, изменения системы негласных следственных действий (статья 231 УПК РК) и обновления Закона «Об оперативно-розыскной деятельности», включая последние поправки, связанные с цифровизацией. Формулируется предложения по дальнейшему совершенствованию правового регулирования межгосударственного розыска лиц.*

Ключевые слова: *розыскная деятельность, оперативно-розыскная деятельность, негласные следственные действия, прерывание сроков досудебного расследования, Уголовного-процессуальный кодекс Республики.*

Введение

Реформа уголовно-процессуального законодательства Республики Казахстан, начатая с введением в действие с 1 января 2015 года нового Уголовно-процессуального кодекса [1], поставила перед теорией и практикой розыскной работы органов внутренних дел ряд вопросов, требовавших законодательного разрешения. В 2016 году автором настоящей статьи была опубликована работа «Правовые режимы розыскной деятельности оперативных подразделений по новому УПК Республики Казахстан» [2], в которой констатировалась, что новая модель уголовного судопроизводства чётко разграничила сферу оперативно-розыскной деятельности (далее-ОРД) и сферу уголовного процесса моментом

регистрации заявления или сообщения в Едином реестре досудебных расследований (далее-ЕРДР), однако оставила неурегулированным вопрос о правовом режиме розыскной работы в период прерывания сроков досудебного расследования-прежде всего в случаях, когда лицо, совершившее уголовное правонарушение, не установлено либо скрылось от органов уголовного преследования.

Цель настоящей статьи-проследить, как данная законодательная неопределённость была разрешена в последующее десятилетие, и на основе анализа действующей редакции уголовно-процессуального и оперативно-розыскного законодательства Республики Казахстан по состоянию на 2026 год сформулировать предложения по дальнейшему совершенствованию правового регулирования.

1.Коллизия 2016 года: краткое напоминание

Суть проблемы, обозначенной автором в 2016 году, состояла в следующем. Согласно концепции нового УПК РК, оперативно-розыскная деятельность в собственном смысле слова (регулируемая Законом РК «Об оперативно-розыскной деятельности» [3]) осуществляется до момента регистрации сообщения в ЕРДР, тогда как после начала досудебного расследования розыск лиц должен обеспечиваться исключительно процессуальными средствами-негласными следственными действиями (глава 30 УПК РК) и розыскными мерами следователя (дознавателя). При этом прямого указания на то, что розыскные мероприятия и негласные следственные действия допустимы также и в период, когда срок досудебного расследования прерваны (то есть формально производство по делу временно не осуществляется), в тексте статьи 45 УПК РК в редакции 2015-2016 годов не содержалось. Это порождало на практике неопределённость: часть правоприменителей толковала прерывание сроков как основание для полного прекращения любых поисковых мероприятий по делу, что явно противоречило бы целям розыска скрывшихся преступников и без вести пропавших лиц.

2.Законодательное решение 2020 года: часть 7-1 статьи 45 УПК РК

Данная коллизия была прямо разрешена Законом Республики Казахстан от 19 декабря 2020 года №384-VI, которым статья 45 УПК РК была дополнена частью 7-1 следующего содержания: «Прерывание сроков досудебного расследования не препятствует проведению по делу необходимых розыскных мероприятий в соответствии с Законом Республики Казахстан «Об оперативно-розыскной деятельности» и негласных следственных действий и приобщению их результатов к материалам уголовного дела» [4]. Формулировка данной нормы примечательно тем, что законодатель прямо допустил продолжение как розыскных мероприятий в рамках Закона «Об ОРД», так и негласных следственных действий в процессуальном режиме-то есть фактически закрепил своего рода «смешанный» правовой режим на период прерывания сроков, сняв ранее существовавшую неопределённость. Тем самым позиция, к которой автор склонялся в 2016 году (о необходимости обеспечить непрерывность розыскной работы независимо от процессуального статуса дела), получила законодательное закрепление.

3.Расширение перечня оснований прерывания сроков (2019-2026 гг.)

Помимо содержательного изменения самого правового режима, за десятилетие существенно расширился и перечень оснований прерывания сроков

досудебного расследования, закреплённый частью седьмой статьи 45 УПК РК. Действующая редакция (с учётом поправок, внесённых законами РК от 27.12.2019 №292-VI, от 19.12.2020 №384-VI, от 27.12.2021 №88-VII, от 05.11.2022 № 157-VII и от 11.06.2026 №307-VIII) включает, помимо оснований, уже известных в 2016 году (неустановление лица, совершившего правонарушения; нахождение подозреваемого, обвиняемого вне пределов Республики Казахстан; их сокрытие от органов уголовного преследования; временное психическое расстройство; необнаружение безвестно исчезнувшего лица), также действие непреодолимой силы и назначение по делу экспертизы [1]. Расширение перечня оснований, вкупе с частью 7-1, свидетельствует о последовательном стремлении законодателя сделать институт прерывания сроков более гибким инструментом, не парализующим розыскную и доказательственную работу по делу.

4.Изменеия системы негласных следственных действий

Параллельно менялся и каталог негласных следственных действий, предусмотренный статьёй 231 УПК РК. Так, Законом РК от 3 июля 2017 года №84-VI был исключён один из первоначальных видов негласных следственных действий, а Законом РК от 27 декабря 2019 года № 292-VI-ещё один [5]. Подобная корректировка перечня негласных следственных действий отражает практику правоприменения первых лет действия нового УПК и постепенную настройку института с учётом выявленных сложностей его использования, в том числе в розыскной работе.

5.Обновление Закона «Об оперативно-розыскной деятельности» от 15 сентября 1994 года №154-XIII также продолжает развиваться.

Последние по времени изменения внесены Законом РК от 17 ноября 2025 года №231- XIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации», вступившим в силу с 18 января 2026 года [6]. В частности, в Закон включена статья 24-1, регламентирующая лицензирование в сфере специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий. Данное дополнение отражает общую тенденцию цифровизации правоохранительной деятельности и требует отдельного осмысления с точки зрения его влияния на розыскную практику органов внутренних дел, в том числе на использование современных технических средств идентификации личности, о чём автором упоминалось в более поздних работах, посвященных новым технологиям в розыскной работе.

6.Нерешённые вопросы и предложения

Несмотря на отмеченные позитивные изменения, за пределами законодательного регулирования по-прежнему остаётся ряд аспектов, обозначенных автором ещё в 2016 году. В частности, сохраняется описанная тогда коллизия «обратного движения» от уголовно-процессуального режима к режиму Закона «Об ОРД» в случае объявления лица в межгосударственный розыск на территории государств-участников Содружества Независимых Государств, поскольку соответствующий Договор государств-участников СНГ о межгосударственном розыске лиц по-прежнему не предусматривает возможности осуществления в его рамках негласных следственных действий. Введение части 7-1

статьи 45 УПК РК данную проблему прямо не затрагивает, поскольку регулирует иную ситуацию-розыск в пределах Республики Казахстан.

В этой связи представляется целесообразным: во-первых, на уровне совместных нормативных актов правоохранительных органов конкретизировать порядок взаимодействия национального и межгосударственного (в рамках СНГ) режимов розыска применительно к части 7-1 статьи 45 УПК РК; во-вторых, продолжить научное осмысление влияния цифровизации оперативно-розыскной деятельности (статья 24-1 Закон «Об ОРД») на розыскную практику; в-третьих, обобщить правоприменительную практику органов внутренних дел по применению части 7-1 статьи 45 УПК РК за период с 2021 по 2026 год, поскольку опубликованных эмпирических исследований по данному вопросу к настоящему времени автору обнаружить не удалость, что само по себе может стать предметом отдельной публикации.

Заключение

Десятилетний период, прошедший с момента публикации автором первой работы по данной теме, показал, что выявленная в 2016 году законодательная неопределённость в вопросе о допустимости розыскных мероприятий и негласных следственных действий в период прерывания сроков досудебного расследования была разрешена законодателем в 2020 году путём введения части 7-1 статьи 45 УПК РК. Вместе с тем развитие законодательства не является завершённым: расширение перечня оснований прерывание сроков, корректировка каталога негласных следственных действий и цифровизация оперативно-розыскной деятельности формирует новую повестку научных исследований в области правового регулирования розыскной работы органов внутренних дел Республики Казахстан.

Список литературы:

1.Уголовно-процесуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V(с изменениями и дополнениями по состоянию на 2026г.) // ИПС «Әділет».- URL: https://adlet.zan.kz/dock/K1400000231

2.Мухамеджанов Е.О. Правовые режимы розыскной деятельности оперативных подразделений по новому УПК Республики Казахстан // Вестник Института законодательства Республики Казахстан. – Астана, 2016.-№1(42).-С.130-133.

3.Закон Республики Казахстан от 15 сентября 1994 года №154-XIII «Об оперативно-розыскной деятельности» (с изменениями и дополнениями по состоянию на 2026г.) // ИПС «Әділет». – URL: URL: https://adilet.zan.kz/rus/docs/Z940004000_

4.О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интелекта и цифровизации: Закон Республики Казахстан от 19 декабря 2020 года №384-VI.

5.О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан: Закон Республики Казахстан от 3 июля 2017 года № 84-VI; Закон Республики Казахстан от 27 декабря 2019 года № 292-VI.

6.О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации: Закон Республики Казахстан от ноября 2025 года №231-VIII.

7.Мухамеджанов Е.О. Правовые основы розыска уголовных преступников и без вести пропавших лиц в период прерывания сроков досудебного расследования // Вестник Института законодательства Ркспублики Казахстан. – Астана, 2016.-№2(43).-С.118-121.

МУХТАРОВ ЭЛЬДАР АЛМАХУНОВИЧ
Начальник кафедры
факультета развития профессиональных компетенций
Академии КНБ Республики Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРЕДУПРЕЖДЕНИИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН: ВОЗМОЖНОСТИ, РИСКИ И ПЕРСПЕКТИВЫ

Стремительная цифровизация общественных и экономических процессов в Республике Казахстан сопровождается расширением использования ИКТ, развитием электронных госуслуг, дистанционных финансовых сервисов и цифровых платформ. Одновременно цифровая трансформация создает новые возможности для противоправных деяний, поскольку значительная часть активности перемещается в цифровую среду. В этих условиях киберпреступность становится одним из значимых вызовов информационной безопасности государства, граждан и организаций.

Актуальность подтверждается динамикой интернет-преступности. По данным Генеральной прокуратуры РК, в 2024 году зарегистрировано 45 156 фактов мошенничества, из которых 22 870 – интернет-мошенничества (+5% к предыдущему году). В первом полугодии 2025 года МВД сообщало о более 11 тыс. случаев интернет-мошенничества, а Антифрод-центр предотвратил хищение свыше 2,6 млрд тенге. Эти показатели свидетельствуют о высокой нагрузке на систему противодействия цифровым преступлениям и необходимости совершенствования механизмов раннего выявления.

Особую сложность представляет усложнение способов совершения киберпреступлений: используются автоматизированные инструменты, социальная инженерия, поддельные цифровые идентификаторы, вредоносное ПО и способы сокрытия следов. Преступная деятельность все чаще приобретает трансграничный характер. Значительная часть интернет-мошенничеств осуществляется транснациональными группами, в том числе с использованием зарубежных call-центров.

Применение ИИ потенциально позволяет осуществлять автоматизированный анализ больших массивов информации, выявлять нетипичные модели поведения, подозрительные транзакции, классифицировать угрозы и формировать прогнозные оценки риска. В правоохранительной деятельности это создает предпосылки для более раннего обнаружения признаков преступной активности и принятия превентивных мер. Однако эффективность таких технологий зависит от качества данных, надежности алгоритмов, защищенности систем ИИ и возможности контроля результатов человеком.

Степень разработанности проблемы характеризуется наличием значительного количества зарубежных исследований по применению ИИ и машинного обучения для обнаружения киберугроз, анализа сетевого поведения, выявления аномалий и прогнозирования преступной активности. Однако казахстанский контекст применения ИИ именно для предупреждения

киберпреступности требует дальнейшего осмысления. Актуально комплексное рассмотрение возможностей технологии одновременно с ее технологическими, организационными, правовыми и этическими ограничениями.

Цифровая трансформация РК сопровождается новыми формами криминальной активности. Перенос финансовых операций, госуслуг, деловой коммуникации в цифровую среду создает дополнительные объекты и каналы для противоправного воздействия. Киберпреступность приобретает характер системного вызова.

Одной из распространенных форм остается интернет-мошенничество. Его специфика – дистанционное воздействие с использованием цифровых каналов и социальной инженерии. Современные схемы позволяют одновременно воздействовать на большое количество жертв, быстро менять инструменты и затруднять установление личности преступника. Опасность представляет сочетание технических атак с психологическим манипулированием. Злоумышленники выдают себя за сотрудников банков, госорганов, правоохранителей, используя поддельные сайты, номера, сообщения. Объектом воздействия становится не только информационная система, но и сам пользователь.

Отдельная проблема – автоматизация для масштабирования преступной деятельности, что снижает затраты и увеличивает масштаб. Киберпреступность характеризуется высокой скоростью трансформации: новые сервисы сопровождаются новыми способами противоправного использования. Система противодействия должна реагировать не только на известные схемы, но и на новые модели поведения.

В этих условиях особое значение приобретает способность правоохранительных органов осуществлять постоянный мониторинг цифровой среды и выявлять признаки опасной активности на ранних этапах. Иначе противодействие сводится к реагированию после причинения ущерба. Для Казахстана это особенно важно из-за развития цифровой экономики и расширения электронных услуг. Чем больше процессов в цифровой среде, тем больше данных, которые являются объектом защиты и источником информации для выявления криминальных закономерностей.

Традиционная модель противодействия ориентирована на обнаружение факта правонарушения, установление обстоятельств, идентификацию виновного и расследование. Она сохраняет значение, но специфика киберпреступности демонстрирует ограничения реактивного подхода. Первое ограничение – объем информации, которую необходимо анализировать. Второе – скорость развития киберугроз. Третье – фрагментарность информации, признаки одной схемы могут находиться в разных системах. Четвертое – необходимость выявления ранее неизвестных моделей поведения, тогда как традиционные системы основаны на заранее определенных признаках или сигнатурах.

Совокупность этих факторов формирует необходимость перехода от реактивного подхода к проактивной модели предупреждения. Внимание переносится с вопроса «какое преступление уже совершено?» на вопросы «какие признаки потенциальной угрозы уже существуют?» и «какие события могут свидетельствовать о подготовке преступления?». В этом контексте ИИ

представляет интерес благодаря способности обрабатывать большие массивы данных, выявлять статистические закономерности и обнаруживать отклонения от типичных моделей поведения. Однако его применение не должно рассматриваться как автоматическая замена специалиста. Более обоснованно использование ИИ как инструмента интеллектуальной поддержки, позволяющего своевременно выделять потенциально значимые события и направлять внимание специалиста на наиболее вероятные риски.

Принципиальное значение имеет анализ поведения. В информационной системе существуют закономерности: временные интервалы активности, типичные объемы операций, используемые устройства, географические параметры подключений, последовательность действий. Существенное отклонение от сформированной модели поведения может быть основанием для дополнительной проверки. Например, отдельная финансовая операция может не содержать признаков мошенничества, но сочетание необычного устройства, нетипичного местоположения, изменения привычного поведения и серии операций формирует более высокий уровень риска. Алгоритмическая обработка таких взаимосвязей позволяет перейти от оценки отдельных событий к комплексному анализу цифрового поведения.

Другое направление – автоматизированный анализ сетевого трафика. Алгоритмы ИИ способны обрабатывать большое количество параметров сетевого взаимодействия и выявлять отклонения, незаметные при ручном анализе. Это актуально в условиях роста количества подключенных устройств и объема информационного обмена.

Следующий уровень – прогнозирование потенциальной преступной активности. Задача – не только ответить, является ли событие подозрительным, но и оценить вероятность возникновения определенного типа угрозы в будущем. Основой прогнозирования выступает анализ исторических данных. При наличии репрезентативного массива информации алгоритмы машинного обучения могут выявлять повторяющиеся закономерности, взаимосвязи между событиями и признаки, статистически связанные с последующим возникновением угроз. Это позволяет формировать прогнозные модели и определять группы событий или ситуаций, требующих повышенного внимания.

В кибербезопасности такой подход может применяться для оценки риска мошеннических операций, выявления потенциально компрометированных аккаунтов, определения подозрительных сетевых взаимодействий и раннего обнаружения признаков координированной преступной активности.

Однако принципиально важно разграничивать прогнозирование риска и предсказание преступника. ИИ не должен использоваться для автоматического признания конкретного лица потенциальным преступником исключительно на основании статистической модели. Прогнозная аналитика должна рассматриваться как инструмент выявления вероятностных сценариев и определения направлений дополнительной проверки.

В казахстанских условиях это особенно важно с точки зрения соблюдения баланса между задачами обеспечения безопасности и защитой прав граждан. Использование прогнозных моделей должно основываться на достоверных данных,

понятных критериях оценки риска и возможности последующего человеческого контроля.

Перспективность прогнозной аналитики заключается также в возможности перехода к риск-ориентированной модели распределения ресурсов. При ограниченном количестве специалистов невозможно одинаково интенсивно анализировать все цифровые события. ИИ может использоваться для первичной оценки большого массива информации и выделения случаев, требующих наиболее оперативного внимания.

Следовательно, прогнозирование с использованием ИИ способно стать следующим этапом развития превентивной кибербезопасности: от фиксации уже произошедшего события — к выявлению вероятных сценариев развития угрозы.

Перспективным направлением является автоматизированное выявление взаимосвязей между событиями. Несколько внешне не связанных инцидентов могут обладать общими признаками: одинаковыми цифровыми инструментами, временными характеристиками, каналами коммуникации. Их автоматизированное сопоставление позволяет сформировать более целостное представление о возможной преступной схеме.

Важное преимущество ИИ – возможность постоянной обработки поступающей информации. В отличие от периодического анализа, проводимого специалистами, автоматизированные системы способны функционировать непрерывно и формировать уведомления при обнаружении заранее определенных или статистически значимых отклонений.

Эффективность таких систем зависит от качества исходных данных. Неполные, противоречивые или некорректные сведения способны привести к ошибочным результатам. Поэтому внедрение ИИ должно сопровождаться развитием стандартов качества данных, механизмов их проверки и процедур контроля результатов алгоритмического анализа.

Отдельного внимания заслуживает проблема объяснимости алгоритмических решений. Некоторые сложные модели ИИ демонстрируют высокую точность, но механизм формирования конкретного результата может быть недостаточно понятен. Для правоохранительной сферы это особенно важно, поскольку аналитический вывод должен не только использоваться на практике, но и поддаваться проверке и обоснованию.

Парадокс современной цифровой безопасности в том, что технология, способная повышать защищенность, одновременно может использоваться для повышения эффективности преступной деятельности. Особую актуальность приобретает распространение генеративного ИИ. Его возможности позволяют автоматизировать подготовку текстов, создание визуального контента, обработку аудио и другие операции, ранее требующие участия человека. В результате снижается порог входа в отдельные виды цифровой преступной деятельности.

ИИ также способен снижать временные и организационные издержки преступников. Автоматизация отдельных этапов подготовки атаки позволяет увеличивать количество целей и быстрее адаптироваться к действиям защитных систем.

Применение ИИ для предупреждения киберпреступности предполагает обработку значительных массивов цифровой информации. В отдельных случаях такая информация может содержать сведения, позволяющие идентифицировать конкретных лиц, характеризующие их поведение, коммуникацию или финансовую активность. Возникает необходимость обеспечения баланса между общественной безопасностью и защитой прав граждан.

Не менее важен вопрос ответственности за ошибочные алгоритмические решения. Если система ИИ сформировала ошибочный сигнал о потенциальной угрозе, необходимо определить, каким образом должен осуществляться последующий контроль и кто несет ответственность за принятое на основании этого сигнала решение.

Рассмотренные возможности и ограничения ИИ позволяют утверждать, что его основное значение для системы противодействия киберпреступности заключается не столько в автоматизации отдельных операций, сколько в возможности изменения самой логики превентивной деятельности. Традиционная модель в значительной степени ориентирована на реагирование после выявления факта преступления. Применение интеллектуальных технологий создает предпосылки для перехода к модели, ориентированной на раннее обнаружение признаков угрозы и оценку вероятности ее дальнейшего развития.

Проактивная модель предполагает непрерывный анализ цифровой среды, при котором потенциально опасные события выявляются еще до того, как они трансформируются в завершенное преступное деяние. Объектом анализа становятся не только уже установленные факты правонарушений, но и совокупность индикаторов, которые могут свидетельствовать о формировании определенной угрозы.

Для Казахстана развитие такого подхода особенно актуально в связи с масштабами цифровизации государственных и финансовых услуг. Чем больше общественно значимых процессов осуществляется посредством цифровых систем, тем выше потенциальная цена несвоевременного обнаружения кибератаки или мошеннической схемы. Следовательно, повышение эффективности предупреждения должно обеспечиваться не только увеличением количества специалистов, но и внедрением инструментов, способных осуществлять масштабный автоматизированный анализ.

В этом отношении ИИ может выполнять функцию аналитического «фильтра», позволяющего выделять из большого массива цифровых событий те, которые характеризуются повышенным уровнем риска. При этом специалист получает возможность сосредоточить внимание не на обработке всего информационного массива, а на наиболее значимых сигналах.

На основании проведенного анализа представляется возможным предложить модель применения ИИ в системе предупреждения киберпреступности, состоящую из семи взаимосвязанных этапов.

Первый этап – сбор и подготовка данных. Формируется массив информации, необходимой для анализа, после чего осуществляется ее структурирование, проверка качества и устранение очевидных ошибок.

Второй этап – интеллектуальный мониторинг. Алгоритмы осуществляют постоянный анализ поступающей информации и фиксируют отклонения от установленных либо сформированных моделей поведения.

Третий этап – выявление аномалий. Определяются события и последовательности действий, которые статистически или поведенчески отличаются от типичных моделей.

Четвертый этап – оценка риска. Выявленным событиям присваивается определенный уровень потенциальной опасности с учетом совокупности имеющихся признаков.

Пятый этап – прогнозирование. На основании выявленных закономерностей формируется оценка возможного дальнейшего развития ситуации.

Шестой этап – экспертная верификация. Специалист проверяет результаты алгоритмического анализа, сопоставляет их с дополнительной информацией и определяет обоснованность сформированного сигнала.

Седьмой этап – превентивное реагирование и обратная связь. В зависимости от результатов проверки принимаются предусмотренные меры, после чего информация об их результатах используется для последующего совершенствования аналитической модели.

Проведенный анализ показывает, что цифровая трансформация РК сопровождается не только расширением возможностей использования информационных технологий, но и усложнением криминогенной среды. Рост объема цифровых данных, распространение дистанционных финансовых сервисов, развитие социальной инженерии и использование автоматизированных инструментов преступниками требуют дальнейшего совершенствования существующих механизмов предупреждения киберпреступности.

Вместе с тем проведенное исследование показывает, что технологические возможности ИИ не следует рассматривать как самостоятельное решение проблемы киберпреступности. Эффективность алгоритмического анализа зависит от качества исходных данных, устойчивости используемых моделей, защищенности информационных систем, квалификации специалистов и наличия соответствующих организационно-правовых механизмов. Дополнительные риски связаны с возможностью использования ИИ самими киберпреступниками для автоматизации и масштабирования противоправной деятельности.

В связи с этим для РК наиболее перспективной представляется проактивная модель предупреждения киберпреступности с использованием ИИ, основанная на сочетании автоматизированного анализа и обязательной экспертной верификации. Такая модель предполагает последовательное прохождение этапов от сбора и обработки данных до выявления аномалий, оценки риска, прогнозирования, экспертной проверки и принятия превентивных мер.

Особое значение при этом приобретает принцип человеческого контроля. ИИ должен выполнять функцию аналитического инструмента, расширяющего возможности специалиста по обработке информации и выявлению потенциальных угроз, но не подменять профессиональное и юридически ответственное принятие решений.

Список литературы:

1. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК. – URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 17.08.2026).
2. Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК. – URL: https://adilet.zan.kz/rus/docs/K2600000255 (дата обращения: 17.08.2026).
3. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. – URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 17.08.2026).
4. Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы: постановление Правительства Республики Казахстан от 28 марта 2023 года № 269. – URL: https://adilet.zan.kz/rus/docs/P2300000269 (дата обращения: 17.08.2026).
5. Gökstorp S., Katsikeas S., Johnson P. Machine Learning for Cybersecurity: A Comprehensive Literature Review // ACM Computing Surveys. – 2026. – Vol. 58, No. 9. – Art. 243. – DOI: 10.1145/3796543.
6. Boateng Y. J., Mim N. J., Akhter N., Naha R., Mahanti A., Barros A. Application of AI in Cyberattack Detection: A Review // Sensors. – 2026. – Vol. 26, No. 5. – Art. 1518. – DOI: 10.3390/s26051518.
7. Huma Z. e., Jan S. U., Ahmad J., Buchanan W., Pitropakis N. Adversarial Machine Learning in IoT Security: A Comprehensive Survey // ACM Computing Surveys. – 2026. – Vol. 58, No. 8. – Art. 202. – DOI: 10.1145/3785665.
8. Pelekis S., Koutroubas T., Blika A., Berdelis A., Karakolis E., Ntanos C., Spiliotis E., Askounis D. et al. Adversarial machine learning: a review of methods, tools, and critical industry sectors // Artificial Intelligence Review. – 2025. – Vol. 58. – Art. 226. – DOI: 10.1007/s10462-025-11147-4.
9. Lee J., Kim S., Park J. Machine Learning for Cybersecurity: A Survey of Applications, Adversarial Challenges, and Future Research Directions // Electronics. – 2025. – Vol. 14, No. 23. – Art. 4563. – DOI: 10.3390/electronics14234563.
10. Vourganas I. J., Michala A. L. Applications of Machine Learning in Cyber Security: A Review // Journal of Cybersecurity and Privacy. – 2024. – Vol. 4, No. 4. – P. 972–992. – DOI: 10.3390/jcp4040045.
11. He K., Kim D. D., Asghar M. R. Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. – 2023. – Vol. 25, No. 1. – P. 538–566. – DOI: 10.1109/COMST.2022.3233793.
12. Macas M., Wu C., Fuertes W. Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Enabled Cybersecurity Systems // Expert Systems with Applications. – 2024. – Vol. 238. – Art. 122223. – DOI: 10.1016/j.eswa.2023.122223.
13. Use of ML and AI in Cybersecurity – A Survey // Procedia Computer Science. – 2024. – Vol. 246. – P. 1260–1270. – DOI: 10.1016/j.procs.2024.09.552.
14. Vulnerabilities in Machine Learning for Cybersecurity: Current Trends and Future Research Directions // Journal of Information Security and Applications. – 2026. – Vol. 96. – Art. 104269. – DOI: 10.1016/j.jisa.2025.104269.
15. Zhou S., Liu C., Ye D., Zhu T., Zhou W., Yu P. S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity // ACM Computing Surveys. – 2022. – Vol. 55, No. 8. – P. 1–39.
16. Bountakas P., Zarras A., Lekidis A., Xenakis C. Defense Strategies for Adversarial Machine Learning: A Survey // Computer Science Review. – 2023. – Vol. 49. – Art. 100573.
17. Jedrzejewski F. V., Thode L., Fischbach J., Gorschek T., Mendez D., Lavesson N. Adversarial Machine Learning in Industry: A Systematic Literature Review // Computers & Security. – 2024. – Vol. 145. – Art. 103988.
18. International Telecommunication Union. Global Cybersecurity Index 2024. – Geneva: ITU, 2024. – URL: https://www.itu.int/ (дата обращения: 17.08.2026).

НИЯЗАЛИЕВ ҚУАНДЫҚ АЛТАЙҰЛЫ
Офицер 17 Департамента 5 Службы
КНБ Республики Казахстан
магистр права
старший лейтенант национальной безопасности,

ҚАЛМҰРАТОВ ӘКІМЖАН АЛМАСҰЛЫ
Консультант 17 Департамента 5 Службы
КНБ Республики Казахстан
магистр права
капитан национальной безопасности

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В ВЫЯВЛЕНИИ СИНТЕЗИРОВАННОЙ И МОДИФИЦИРОВАННОЙ РЕЧИ: ПРОБЛЕМЫ DEEPFAKE И SPOOFING

Генеративный искусственный интеллект за последние годы сильно изменил подходы к созданию и обработке речевого контента. Системы синтеза речи научились формировать высказывания, которые звучат вполне естественно, воспроизводить голосовые особенности конкретного человека и перекладывать исходную речь на нужный язык или интонацию. Раньше для убедительной подделки голоса нужны были большие массивы записей и специальное оборудование – сегодня подобные инструменты доступны практически любому пользователю. Наряду с полезными применениями в сфере доступности, образования, медиапроизводства и голосовых интерфейсов это порождает и новые риски: искусственно созданную речь всё чаще используют в противоправных целях [1, 2].

Для криминалистики эта проблема стоит особенно остро. Традиционно аудиозапись рассматривалась как источник сведений о самом событии, обстоятельствах разговора и личности говорящего. Но с развитием технологий клонирования голоса перед экспертом встаёт дополнительный вопрос: перед ним запись естественной речи или она полностью либо частично сгенерирована, преобразована или смонтирована с помощью алгоритмов ИИ? Задачи фоноскопической экспертизы в связи с этим расширяются – теперь нужно ещё и выявлять признаки искусственного происхождения речи, а также оценивать, насколько надёжны автоматизированные средства такого выявления.

Цель настоящей работы – рассмотреть, что современный искусственный интеллект может предложить для выявления синтезированной и модифицированной речи, обозначить основные ограничения существующих подходов и наметить перспективы их применения в фоноскопических исследованиях.

Искусственную речь получают в основном двумя способами: синтезом по тексту (Text-to-Speech, TTS) и преобразованием голоса (Voice Conversion, VC). В первом случае акустический сигнал генерируется на основе заданного текста, во втором — характеристики уже существующей записи меняются так, чтобы она воспринималась как голос другого человека. Современные алгоритмы неплохо

справляются с воспроизведением тембра, манеры произношения, интонации и прочих индивидуальных особенностей речи. Отдельно стоит voice cloning – построение модели голоса конкретного человека по имеющимся образцам его речи [1, 3].

В научной литературе для такой искусственно созданной или изменённой речи закрепилось понятие speech (audio) deepfake. При этом deepfake и spoofing – не одно и то же, и их стоит разграничивать. Deepfake – это, прежде всего, способ и результат искусственного создания или значительного преобразования контента. Spoofing же обозначает использование поддельного сигнала для того, чтобы выдать себя за настоящего пользователя или обмануть систему идентификации. То есть синтезированный голос сам по себе – уже deepfake-контент, а вот его предъявление системе голосовой биометрии от имени другого человека – это уже spoofing-атака. Международная инициатива ASVspoof изучает, помимо прочего, атаки с использованием TTS, VC и повторного воспроизведения записей, а также разрабатывает контрмеры для отличия подлинной речи от поддельной [4].

Насколько это реальная угроза, а не гипотетическая. Случаи voice-fraud уже неоднократно фиксировались на практике. В 2019 году мошенники, синтезировав голос гендиректора немецкой материнской компании, убедили руководителя её британского подразделения перевести около 243 тысяч долларов на подставной счёт – этот инцидент считается одним из первых задокументированных случаев голосового deepfake-мошенничества в корпоративной среде. В 2024 году сотрудник финансового отдела гонконгского подразделения крупной международной компании перевёл мошенникам порядка 25 миллионов долларов после видеоконференции, на которой все «участники», включая якобы финансового директора, оказались синтезированными с помощью ИИ. По оценке Juniper Research, суммарные потери от мошенничества с клонированием голоса в мире могли превысить 300 миллионов долларов уже к 2025 году, причём эта цифра, вероятно, занижена – значительная часть подобных инцидентов остаётся незафиксированной или неквалифицированной именно как voice-deepfake атака [7, 8].

Рост качества генеративных моделей расширяет и спектр угроз, значимых для криминалистики. Искусственно созданную речь применяют при телефонном мошенничестве, для имитации голоса родственника, начальника или другого доверенного лица, для обхода голосовой биометрии, распространения ложных сообщений и создания аудиозаписей, которые внешне выглядят подлинными. Причём речь не только о полностью сгенерированной фонограмме – возможна и локальная замена отдельных слов или фрагментов, что серьёзно усложняет установление факта вмешательства.

С криминалистической точки зрения важно понимать: убедительность записи для слушателя ещё ничего не говорит о её подлинности. Обзоры современных исследований показывают, что человеческое восприятие само по себе довольно ненадёжно, когда речь идёт о распознавании качественной синтетической речи. Поэтому слуховой анализ должен обязательно дополняться инструментальными методами исследования сигнала и автоматизированными алгоритмами поиска аномалий [1, 2].

В основе автоматического обнаружения синтезированной речи лежит поиск признаков, которые оставляют после себя алгоритмы генерации или преобразования сигнала. Такие следы могут проявляться в спектральной структуре, динамике основной частоты, временной организации речи, фазовых характеристиках, особенностях высоких частот, переходных участках, паузах и других параметрах. Проблема в том, что по мере развития генераторов эти артефакты становятся всё менее выраженными. Из-за этого современные системы обнаружения всё больше полагаются на глубокие нейронные сети и признаки, которые извлекаются автоматически прямо из речевого сигнала.

Типичная система обнаружения deepfake-речи работает в три этапа: предварительная обработка фонограммы, извлечение информативных признаков и, наконец, классификация сигнала как подлинного либо искусственного. В качестве входных данных могут использоваться спектрограммы, кепстральные и другие акустические признаки, а также признаки, которые извлекают предварительно обученные речевые модели. Классификатор ищет совокупность закономерностей, статистически отличающих естественную речь от синтезированной или преобразованной [2, 3].

Эволюция архитектур детекторов. Заметный вклад в развитие этого направления внесла серия международных исследований ASVspoof. В рамках ASVspoof 2021 были выделены три отдельных сценария: Logical Access, Physical Access и Speech Deepfake. Logical Access касался речи, сформированной с помощью TTS и VC и переданной по телефонным и VoIP-каналам; Physical Access был посвящён атакам повторного воспроизведения в реальных акустических условиях; Speech Deepfake – непосредственно различению естественных и искусственно сформированных записей. Базовые решения того поколения – LFCC-GMM, CQCC-GMM, LFCC-LCNN и RawNet2 – опирались на классические акустические признаки и относительно неглубокие модели [4, 5].

С тех пор архитектуры заметно продвинулись вперёд. Модель AASIST (Audio Anti-Spoofing using Integrated Spectro-Temporal Graph Attention Networks), объединяющая спектральный и временной графы сигнала через механизм графового внимания, показала EER около 0,83% на наборе ASVspoof2019 LA – заметный шаг вперёд по сравнению с более ранними решениями. Дальнейшее улучшение дало использование самообучаемых (self-supervised, SSL) речевых представлений: замена классического фронт-энда на предобученную модель wav2vec 2.0 в сочетании с AASIST и методом аугментации данных RawBoost позволила снизить EER до 0,82% на ASVspoof2021 LA и до 2,85% на сценарии Speech Deepfake того же набора – это одни из наиболее низких показателей ошибки, зафиксированных в литературе на момент публикации. С 2024–2025 годов исследования проводятся уже на более новом наборе ASVspoof5, приближенном к условиям «в дикой природе» (разнообразные кодеки, каналы передачи, шум), а последующие модификации AASIST с SSL-фронт-эндом фиксируют на нём EER порядка 7-8% – рост ошибки по сравнению с лабораторными наборами хорошо иллюстрирует, насколько сильно условия записи и передачи влияют на реальную эффективность детектора [4, 5, 9].

Вместе с тем высокая точность алгоритма на тестовом наборе данных совсем не гарантирует, что он одинаково хорошо подойдёт для практической экспертизы. Одна из главных проблем – обобщающая способность модели. Детектор может уверенно распознавать способы генерации, которые встречались в обучающей выборке, и при этом заметно хуже справляться с новым синтезатором, незнакомым вокодером, другим языком, иными условиями записи или способом передачи фонограммы. Показательный пример даёт одна из недавних работ по частичным deepfake: модель, обученная и протестированная на одном и том же наборе (PartialSpoof), даёт EER около 2,5%, но при переносе на другой набор с иным способом монтажа речи (PartialEdit) ошибка вырастает до 23-24% – почти в десять раз. Современные обзоры относят межнаборную переносимость, обнаружение ранее неизвестных атак и устойчивость к изменению условий сигнала к числу ключевых нерешённых задач в области deepfake detection [2, 3, 9].

Для криминалистической практики эта проблема стоит особенно остро, поскольку исследуемые фонограммы редко поступают в лабораторном качестве. Запись могла неоднократно перекодироваться, пересылаться через мессенджеры, записываться с громкой связи, содержать реверберацию, фоновые шумы, наложенную речь и другие искажения. Всё это способно замаскировать те самые низкоуровневые артефакты, по которым модель училась распознавать синтез. Исследования устойчивости показывают, что эффективность отдельных детекторов заметно падает при смене кодеков, генеративных моделей и наборов данных [6].

Частичный deepfake: от классификации к локализации. Дополнительную сложность создаёт частичный deepfake – когда искусственно сформирован не весь сигнал, а лишь отдельный фрагмент, а остальная часть записи остаётся подлинной. Для изучения этой задачи созданы специализированные наборы данных: PartialSpoof, где случайные сегменты подлинной речи заменяются синтезированными фрагментами разной длины и предоставляются метки на уровне отдельных сегментов, а не всей записи целиком; Half-Truth (HAD), где заменяются отдельные слова – имена, названия мест, организаций, даты; ADD 2022/2023 с отдельным треком PSAL (Partially Spoofed Audio Localization), нацеленным именно на определение границ подделанного участка, а не только факта его наличия. Методически задача решается двумя основными способами: покадровой (frame-level) разметкой, когда модель присваивает метку каждому короткому отрезку сигнала, и двухэтапными схемами, где сначала определяются границы перехода между подлинным и синтезированным участком (boundary detection), а затем каждый выделенный сегмент оценивается отдельно. У обоих подходов есть свои ограничения: покадровая разметка теряет контекст при уменьшении длины кадра, а модели, обученные на явных признаках монтажных склеек, плохо переносятся на более совершенные методы нейросетевого редактирования речи, где такие склейки практически не оставляют следов [2, 9]. Для экспертной практики это означает, что даже успешная бинарная классификация всей фонограммы не снимает вопроса о том, где именно проходит граница между подлинным и искусственным материалом.

При оценке возможностей искусственного интеллекта необходимо также учитывать проблему интерпретируемости. Нейросетевая модель способна выдать высокий показатель вероятности принадлежности записи к классу deepfake, однако

для экспертной деятельности принципиально важно понимать, на основании каких устойчивых признаков получен такой результат, насколько он зависит от конкретной модели и может ли быть воспроизведен при повторном исследовании. Поэтому автоматическая классификация не должна механически подменять комплексное исследование фонограммы.

Процессуальный аспект. Отдельного рассмотрения требует статус результата работы ИИ-детектора как источника доказательственной информации. В отличие от традиционных инструментальных методов фоноскопии, нейросетевая модель – это, по существу, «чёрный ящик» с постоянно меняющейся версией и параметрами обучения, что создаёт трудности для соблюдения требований воспроизводимости и проверяемости методики, обычно предъявляемых к экспертному заключению. Практически это означает необходимость фиксировать в заключении не только итоговый вывод, но и версию модели, набор данных, на котором она обучена и валидирована, показатели её точности на независимых наборах, а также границы её применимости – во избежание ситуации, когда автоматическая оценка вероятности синтеза представляется суду как безусловный факт. Разработка единого методического стандарта для описания и представления таких результатов – отдельная и пока не решённая задача, требующая координации между разработчиками детекторов и судебно-экспертным сообществом.

Представляется обоснованным рассматривать искусственный интеллект как дополнительный инструмент специалиста, а не как самостоятельное решение. Результат работы детектора может использоваться для первичного скрининга, поиска подозрительных участков и формирования направлений дальнейшего инструментального анализа. Окончательная оценка должна осуществляться с учетом качества и происхождения записи, условий ее получения, возможного перекодирования, длительности речевого материала, характеристик диктора, результатов акустического анализа и иных обстоятельств конкретного исследования.

Отдельного внимания требует вопрос языковой и речевой специфики. Большинство известных наборов данных формируется в определенных языковых условиях, тогда как реальная практика может включать казахскую, русскую и смешанную казахско-русскую речь, переключение языковых кодов, региональные особенности произношения и современную разговорную лексику. Модель, обученная преимущественно на одном языке и ограниченном наборе дикторов, не должна автоматически считаться одинаково надежной для иной языковой среды. Следовательно, перспективным направлением является формирование репрезентативных отечественных наборов естественной, синтезированной и преобразованной речи с учетом различных каналов записи и передачи.

Такие наборы целесообразно формировать не только по принципу «подлинная/синтетическая речь», но и с учетом способа генерации, примененного кодека, характеристик канала связи, уровня фонового шума, длительности речевого фрагмента и языка. Это позволит проводить контролируемую апробацию программных решений и определять границы их применимости. Не менее важным является включение в тестирование ранее не использовавшихся при обучении

алгоритмов синтеза, поскольку именно такой сценарий наиболее близок к реальной экспертной ситуации.

Перспективы внедрения ИИ в фоноскопические исследования связаны с созданием многоуровневых систем, в которых автоматический анализ не ограничивается выдачей бинарного результата. Практически значимая система должна указывать степень уверенности, локализовать подозрительные фрагменты, предоставлять исследователю визуализируемые признаки, фиксировать версию модели и параметры анализа, а также обеспечивать воспроизводимость процедуры. Подобный подход позволит приблизить технологии deepfake detection к требованиям, предъявляемым к инструментальным методам криминалистического исследования.

Необходимым условием также является постоянное обновление программно-технических средств. В отличие от многих традиционных объектов исследования, характеристики синтезированной речи быстро изменяются вместе с развитием генеративных моделей. Детектор, показавший высокую эффективность в отношении технологий одного поколения, может оказаться недостаточно чувствительным к новым способам синтеза. По этой причине внедрение должно сопровождаться периодической валидацией, тестированием на актуальных образцах, накоплением собственных данных и повышением квалификации специалистов.

Таким образом, развитие технологий синтеза и преобразования голоса формирует качественно новый класс объектов фоноскопического исследования. Современные системы искусственного интеллекта способны выявлять статистические и акустические закономерности, характерные для искусственно сформированной речи, и уже демонстрируют значительный потенциал в задачах anti-spoofing и speech deepfake detection. Одновременно сохраняются существенные ограничения, связанные с неизвестными алгоритмами генерации, качеством фонограммы, воздействием кодеков и каналов передачи, языковой спецификой, частичными модификациями, недостаточной интерпретируемостью отдельных моделей и отсутствием единых процессуальных стандартов представления результатов автоматизированного анализа.

В этих условиях наиболее перспективной представляется модель применения искусственного интеллекта, при которой автоматизированные средства дополняют, а не заменяют профессиональную деятельность специалиста. Для практического внедрения необходимы апробированные методические подходы, специализированные наборы данных, регулярная оценка устойчивости алгоритмов, методические стандарты фиксации результатов и подготовка специалистов, способных интерпретировать результаты машинного анализа. Особую актуальность имеет проведение исследований на материале казахской, русской и смешанной речи, что позволит оценить применимость современных методов к национальной криминалистической практике и сформировать научно-методическую основу для дальнейшего развития данного направления.

Список литературы:

1. Zhang B., Cui H., Nguyen V., Whitty M. Audio Deepfake Detection: What Has Been Achieved and What Lies Ahead // Sensors. 2025. Vol. 25. Art. 1989. DOI: 10.3390/s25071989.
2. Li M., Ahmadiadli Y., Zhang X.-P. A Survey on Speech Deepfake Detection // ACM Computing Surveys. 2025. Vol. 57, No. 7. Art. 165. DOI: 10.1145/3714458.
3. Pham L. et al. A Comprehensive Survey with Critical Analysis for Deepfake Speech Detection // Computer Science Review. 2025. Vol. 57. Art. 100757. DOI: 10.1016/j.cosrev.2025.100757.
4. ASVspoof 2021 Evaluation Plan. Automatic Speaker Verification Spoofing and Countermeasures Challenge, 2021.
5. ASVspoof 2021: Challenge databases, baselines and post-challenge resources. ASVspoof official project website.
6. Robustness in deepfake speech detection: A survey of failure mechanisms including an experimental case study // Computer Speech & Language. 2026.
7. Инцидент с британским подразделением немецкой энергетической компании (2019) – один из первых задокументированных случаев корпоративного мошенничества с использованием синтезированного голоса.
8. Оценка потерь от voice-cloning fraud — Juniper Research (прогноз свыше 300 млн долл. к 2025 г.).
9. Работы по архитектурам AASIST, wav2vec2.0-SSL и наборам PartialSpoof/PartialEdit/HAD (ASVspoof consortium; исследования по обнаружению и локализации частичных deepfake, 2021–2026).

ОЛЕКСЮК МАКСИМ ВЯЧЕСЛАВОВИЧ
Доцент кафедры уголовно-исполнительного права
Костанайской академии МВД Республики Казахстан имени Ш.Кабылбаева
доктор философии (PhD), подполковник полиции

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕХАНИЗМЫ ВНЕДРЕНИЯ И КОНТРОЛЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Стремительное развитие технологий искусственного интеллекта (далее – ИИ) кардинально трансформирует различные сферы государственного управления, включая правоохранительную деятельность. Системы видеоаналитики, биометрической идентификации, предиктивной аналитики и автоматизированной обработки больших данных все активнее внедряются в работу полиции, органов уголовного преследования и иных субъектов правоохранительной системы. Республика Казахстан, взявшая курс на цифровую трансформацию государственного управления, не осталась в стороне от этого процесса. Так, 17 ноября 2025 года Президентом Республики Казахстан был подписан Закон «Об искусственном интеллекте», ставший первым специализированным актом такого рода в центральноазиатском регионе [1].

Актуальность темы обусловлена противоречием между объективной потребностью правоохранительных органов в использовании передовых цифровых инструментов для повышения эффективности профилактики, раскрытия и расследования правонарушений, с одной стороны, и необходимостью обеспечения конституционных прав и свобод человека, презумпции невиновности, неприкосновенности частной жизни и защиты персональных данных с другой. Отсутствие до недавнего времени системного правового регулирования порождало риски бесконтрольного расширения технологий массового видеонаблюдения и биометрической идентификации, на что указывалось экспертным сообществом ещё на стадии обсуждения Концепции развития искусственного интеллекта [2].

До 2024 года отношения, связанные с использованием технологий искусственного интеллекта в Республике Казахстан, специальным образом не регулировались. Соответствующие вопросы затрагивались лишь опосредованно, в рамках общего законодательства об информатизации и о персональных данных и их защите [3; 4], которое оперирует общими категориями персональных и биометрических данных и не содержит понятий, отражающих специфику систем искусственного интеллекта и алгоритмического принятия решений. Ситуация начала меняться с принятием Правительством Республики Казахстан постановления «Об утверждении Концепции развития искусственного интеллекта на 2024-2029 годы», разработанного Министерством цифрового развития, инноваций и аэрокосмической промышленности [5]. Документ закрепил систему принципов государственной политики в сфере ИИ, включая ответственность, приоритет человека в процессе принятия решений, прозрачность и справедливость, управление рисками, безопасность и конфиденциальность, а также принцип адаптивного регулирования, предполагающий поэтапное повышение уровня

регулирования по мере развития технологий [5]. Среди целевых индикаторов Концепции – рост доли организаций высшего, послевузовского, технического и профессионального образования, включивших дисциплины по искусственному интеллекту в образовательные программы, с 20% в 2025 году до 60% в 2029 году [5], а также формирование Национальной сборной ИИ из казахстанских специалистов, работающих в международных технологических компаниях.

Экспертное сообщество, в частности эксперты Евразийского Цифрового Фонда, участвующие в диалоге с государством на площадке Digital Rights Asia, уже на этапе обсуждения Концепции сформулировало ряд рекомендаций, имеющих прямое отношение к правоохранительной сфере. В числе таких положений, непосредственно связанных с правоохранительной деятельностью следует выделить запрет массовой и неизбирательной слежки посредством систем видеонаблюдения; запрет на использование систем биометрической идентификации в реальном времени для любых субъектов, кроме правоохранительных органов; категоризация биометрических систем по уровню риска по аналогии с подходом, применяемым в Европейском союзе [2]. Данные предложения фактически предвосхитили последующее законодательное решение о выделении правоохранительной деятельности в качестве отдельной, повышенно чувствительной сферы применения ИИ.

Ключевым актом остаётся Закон Республики Казахстан «Об искусственном интеллекте», введённый в действие 18 января 2026 года [6]. Закон закрепляет понятийный аппарат, в частности, искусственный интеллект определяется как функциональная способность к имитации когнитивных функций, характерных для человека, обеспечивающая результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их, а также устанавливает систему принципов государственного регулирования отношений в сфере ИИ, включающую законность, справедливость и равенство, прозрачность и объяснимость, ответственность и подконтрольность, приоритет благополучия человека, защиту данных и конфиденциальности, безопасность и защищённость [6]. Статья 18 Закона вводит институт управления рисками систем искусственного интеллекта, а статья 21 закрепляет обязательную маркировку синтетических результатов деятельности систем ИИ – изображений, видео, аудио и текстов, имитирующих внешность, голос или поведение физического лица либо не происходившие в действительности события [6]. Одновременно с базовым законом принят Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации», которым синхронно скорректированы законодательство о персональных данных и их защите, об информатизации, об оперативно-розыскной деятельности, о защите прав потребителей, о разрешениях и уведомлениях, а также ряд иных законодательных актов [7].

Организационное обеспечение реализации указанных законов возложено на центральные государственные органы. Распоряжением Премьер-Министра Республики Казахстан от 14 января 2026 года № 2-р утверждён перечень подзаконных нормативных правовых актов, подлежащих разработке во исполнение

законов об ИИ, установлена обязанность профильных министерств и ведомств ежемесячно, не позднее 30 числа, размещать на общедоступном государственном объекте информатизации сведения о ходе нормотворческой работы, а Министерству юстиции Республики Казахстан поручено ежемесячно, не позднее 5 числа, анализировать, обобщать и публиковать сводную информацию о реализации данных законов. [8]. Тем самым сформирован организационный механизм поэтапного и контролируемого внедрения детального регулирования – от рамочного закона к системе ведомственных актов.

Институциональной основой цифровой трансформации выступает Министерство искусственного интеллекта и цифрового развития Республики Казахстан [1]. Принятие Закона «Об искусственном интеллекте» сопровождалось введением в действие в тот же день сопутствующего Закона № 231-VIII, которым внесены изменения в одиннадцать законодательных актов различной отраслевой принадлежности: об оперативно-розыскной деятельности, об органах национальной безопасности, о регулировании торговой деятельности, о связи, о защите прав потребителей, о персональных данных и их защите, о разрешениях и уведомлениях, об информатизации, о почте, о цифровых активах и о масс-медиа [7], что подтверждает комплексный, системный характер организационно-правовой реформы. На уровне взаимодействия с органами внутренних дел организационный механизм может быть представлен несколькими уровнями: во-первых, стратегическим – определением приоритетных направлений цифровизации в рамках Концепции 2024–2029 годов, в ходе обсуждения которой Премьер-Министром Республики Казахстан государственное управление было названо в числе приоритетных отраслей внедрения искусственного интеллекта наряду с субъектами естественных монополий в нефтегазовой, горнодобывающей, энергетической, транспортной, логистической, водоснабжающей и сельскохозяйственной отраслях [9]; во-вторых, нормативным – принятием ведомственных актов, регламентирующих порядок эксплуатации конкретных систем ИИ; в-третьих, операционным – непосредственным развёртыванием и эксплуатацией интеллектуальных систем силами территориальных подразделений полиции совместно с операторами цифровой инфраструктуры городов.

Важным элементом организационного механизма стало внесение изменений в статью 31 Кодекса Республики Казахстан об административных правонарушениях в рамках Цифрового кодекса: с 28 апреля 2026 года расширены возможности автоматической фиксации правонарушений интеллектуальными системами – если ранее использование телефона за рулём или отсутствие ремня безопасности фиксировались исключительно сотрудником полиции на дороге, то теперь это может осуществляться автоматизированными системами видеоаналитики [10]. Подобное решение потребовало создания организационных процедур верификации результатов автоматической фиксации, порядка обжалования и распределения ответственности между оператором технической системы и уполномоченным должностным лицом органа внутренних дел.

Наиболее масштабным примером внедрения ИИ в сферу общественной безопасности выступает развитие сети интеллектуального видеонаблюдения.

К маю 2026 года, согласно данным, представленным заместителем Премьер-министра – министром культуры и информации Республики Казахстан А. Балаевой в ответ на запрос сенаторов, число таких камер превысило 43 тысячи, а количество применяемых видов видеоаналитики достигло 35, включая алгоритмы, анализирующие поведение людей [11].

Показательным примером регионального уровня является интеллектуальная система видеонаблюдения «Таргет-Ай», внедрённая в Бурабайском районе Акмолинской области. Система, построенная на алгоритмах искусственного интеллекта, автоматически распознаёт лица, номерные знаки автомобилей и фиксирует аномальное поведение, что, по оценке органов внутренних дел, за первые три месяца эксплуатации ускорило реагирование полиции на происшествия и повысило качество оперативных решений [12]. Отдельным направлением выступает внедряемая система розыска транспортных средств, в отношении которых наложен запрет на эксплуатацию в связи с неисполненными обязательствами их владельцев: посредством городских камер видеонаблюдения и искусственного интеллекта сведения о таких машинах будут передаваться подразделениям полиции для их изъятия и помещения на специализированные стоянки [13].

Приведённые примеры свидетельствуют, что практика внедрения ИИ в правоохранительную деятельность Казахстана существенно опередила темпы формирования специализированного правового регулирования. Базовый Закон «Об искусственном интеллекте» вступил в силу лишь в январе 2026 года, тогда как соответствующие технологические решения эксплуатируются на протяжении нескольких лет. Это актуализирует задачу ретроспективной правовой оценки уже развёрнутых систем и приведения условий их эксплуатации в соответствие с новыми законодательными требованиями.

Отправной точкой для построения механизмов контроля выступают конституционные положения о неприкосновенности частной жизни, личной и семейной тайны, а также о защите чести и достоинства человека, которые в равной мере распространяются на отношения, связанные с автоматизированной обработкой персональных данных правоохранительными органами [14]. На данной конституционной основе Закон «Об искусственном интеллекте» формирует несколько взаимодополняющих механизмов контроля. Во-первых, это дифференциация систем ИИ по степени риска для прав и свобод человека, закреплённая в статье 17, и связанный с ней институт управления рисками (статья 18), предполагающий выявление, оценку и устранение рисков на протяжении всего жизненного цикла системы; повышенные требования к системам высокого риска по своей природе распространяются на подавляющее большинство правоохранительных приложений – биометрическую идентификацию, предиктивную аналитику, автоматическую фиксацию правонарушений [6]. Во-вторых, статья 8 закона устанавливает, что все субъекты, занимающиеся созданием и эксплуатацией систем ИИ, несут ответственность за деятельность таких систем и за результаты их деятельности на всех этапах жизненного цикла, исходя из своей роли. Данная норма распространяет ответственность не только на разработчика, но и на оператора, использующего систему в оперативно-служебной деятельности [6].

Важным правовым ограничителем выступает законодательство о персональных данных. Закон Республики Казахстан «О персональных данных и их защите» устанавливает для операторов, к числу которых относятся и правоохранительные органы, обязанность утверждать перечень обрабатываемых персональных данных, документы, определяющие политику их сбора, обработки и защиты, а также принимать необходимые правовые, организационные и технические меры защиты [4]. Одновременно закон допускает обработку персональных данных без согласия субъекта в целях защиты конституционных прав и свобод человека и гражданина, если получение такого согласия невозможно, что применимо к оперативно-разыскной и уголовно-процессуальной деятельности, однако требует строгого, ограничительного толкования во избежание расширительного применения данного основания [4].

Ещё одним элементом механизма контроля является обязательная маркировка синтетического контента, создаваемого системами ИИ, что имеет значение для оценки допустимости использования материалов видеоаналитики и биометрической идентификации в качестве доказательств в уголовном процессе с точки зрения требований Уголовно-процессуального кодекса Республики Казахстан к относимости, допустимости и достоверности доказательств [15]. Установленная законом ответственность за нарушение законодательства в сфере искусственного интеллекта дополняет систему прокурорского надзора и судебного контроля за законностью применения технических средств в правоохранительной деятельности, формируя, таким образом, многоуровневую систему сдержек – ведомственный контроль, вневедомственный (прокурорский) надзор и судебную проверку законности использования полученных данных.

Несмотря на формирование базового правового каркаса, сохраняется ряд системных проблем. Первая проблема это темпоральный разрыв между практикой применения технологий и их правовым регулированием: системы массового видеонаблюдения и биометрической идентификации функционируют в правоохранительной сфере Казахстана уже несколько лет, тогда как специальное регулирование появилось лишь в 2025-2026 годах [6; 11]. Вторая проблема связана с недостаточной проработанностью механизмов независимого аудита алгоритмов, используемых правоохранительными органами, включая оценку точности распознавания лиц, риск ложных срабатываний и потенциальную алгоритмическую дискриминацию по демографическим признакам. Третья проблема – размытость границ между использованием ИИ для профилактики правонарушений и элементами предиктивной полицейской деятельности, которая при отсутствии чётких критериев способна вступать в противоречие с презумпцией невиновности и принципом индивидуализации ответственности.

Четвёртая проблема носит организационный характер и связана с распределением компетенции между Министерством искусственного интеллекта и цифрового развития, Министерством внутренних дел, местными исполнительными органами и частными операторами цифровой инфраструктуры городов, эксплуатирующими системы городского видеонаблюдения, что порождает риски размывания ответственности за качество и законность работы конкретных систем [12]. Наконец, сохраняется потребность в развитии процессуальных гарантий:

чёткого порядка обжалования решений, принятых или подготовленных с использованием систем ИИ, включая случаи автоматической фиксации административных правонарушений [10], а также права лица знать о применении в отношении него технологий биометрической идентификации, что прямо согласуется с ранее сформулированными рекомендациями экспертного сообщества об ограничении применения биометрической идентификации в реальном времени исключительно правоохранительными органами и о категоризации таких систем по уровню риска [2].

С учётом изложенного представляется целесообразным предложить следующие меры совершенствования организационно-правовых механизмов внедрения и контроля ИИ в правоохранительной деятельности Республики Казахстан.

Во-первых, разработать и принять специализированный ведомственный акт Министерства внутренних дел Республики Казахстан, устанавливающий закрытый перечень допустимых к применению систем ИИ высокого риска в правоохранительной деятельности, а также порядок их сертификации и включения в соответствующий реестр в рамках подзаконных актов, разрабатываемых во исполнение законов об искусственном интеллекте.

Во-вторых, закрепить обязательность независимой технической экспертизы (аудита) алгоритмов распознавания лиц и предиктивной аналитики до их внедрения в оперативно-служебную деятельность с периодической переаттестацией уже эксплуатируемых систем.

В-третьих, установить в уголовно-процессуальном и административно-деликтном законодательстве порядок использования данных, полученных с применением систем ИИ, в качестве доказательств, включая обязательное указание на факт автоматизированной обработки и право стороны защиты на оспаривание достоверности таких данных.

В-четвертых, создать механизм ведомственного и вневедомственного (прокурорского) контроля за соблюдением требований законодательства о персональных данных при эксплуатации систем видеонаблюдения и биометрической идентификации, включая регулярную публичную отчётность по аналогии с уже установленной практикой ежемесячного информирования о ходе реализации законодательства об ИИ.

И, наконец, в-пятых, внедрить принцип «человек в контуре принятия решения» применительно к юридически значимым решениям, затрагивающим права граждан, исключив полностью автоматизированное привлечение к ответственности без верификации результатов работы системы ИИ уполномоченным должностным лицом.

Проведённый анализ показывает, что в Республике Казахстан за период 2024-2026 годов сформирована базовая организационно-правовая инфраструктура регулирования искусственного интеллекта, кульминацией которой стало принятие Закона «Об искусственном интеллекте» – первого подобного акта в Центральной Азии. Вместе с тем практика опережающего внедрения технологий видеоаналитики и биометрической идентификации в деятельность правоохранительных органов обусловливает необходимость дальнейшей детализации механизмов контроля:

развития института независимого аудита алгоритмов, процессуальных гарантий использования результатов работы ИИ в доказывании, а также чёткого разграничения компетенции между государственными органами и частными операторами цифровой инфраструктуры. Совершенствование организационно-правовых механизмов в данной сфере должно осуществляться на основе баланса между повышением эффективности правоохранительной деятельности и безусловным обеспечением конституционных прав и свобод человека и гражданина.

Список литературы:

1. Казахстан принял первый в Центральной Азии Закон об искусственном интеллекте // Мин-во ИИ и цифрового развития РК. 17.11.2025. gov.kz/memleket/entities/maidd/press/news/details/1106455

2. Правительство Казахстана представило концепцию развития искусственного интеллекта // Digital Rights Asia. 18.07.2024. digitalrights.asia/events/concept-for-the-development-of-ai

3. Обзор изменений законодательства в сфере персональных данных в РК на 2024 год // Internews. 14.03.2024. greaterinternetfreedom.org

4. О персональных данных и их защите: Закон РК от 21.05.2013 № 94-V // ИПС «Әділет». adilet.zan.kz/rus/docs/Z1300000094

5. Об утверждении Концепции развития ИИ на 2024-2029 годы: Постановление Правительства РК от 24.07.2024 № 592 // ИПС «Әділет». adilet.zan.kz/rus/docs/P2400000592

6. Об искусственном интеллекте: Закон РК от 17.11.2025 № 230-VIII ЗРК // ИПС «Әділет». adilet.zan.kz/rus/docs/Z2500000230

7. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации: Закон Республики Казахстан от 17 ноября 205 года № 231-VIII ЗРК // https://www.adilet.zan.kz/rus/docs/Z2500000231

8. О мерах по реализации законов Республики Казахстан от 17 ноября 2025 года «Об искусственном интеллекте» и «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам искусственного интеллекта и цифровизации»: распоряжение Премьер-Министра Республики Казахстан от 14 января 2026 года № 2-р (документ на ИПС «Әділет»: adilet.zan.kz/rus/docs/R2600000002) .

9. Концепцию развития ИИ на 2024-2029 годы приняли в правительстве // Kapital.kz. 16.07.2024. kapital.kz/tehnology/127701

10. Системы, которые «понимают»: как работает технология распознавания лиц и зачем она городу // 365info.kz. 28.04.2026

11. Более 19 тысяч видеокамер с ИИ установлено в Казахстане // 24.kz. 29.08.2025

12. Как искусственный интеллект помогает полиции раскрывать преступления // BAQ.KZ. 30.08.2025

13. В Казахстане городские камеры оснастили функцией распознавания лиц должников // BES.media. 19.09.2025

14. Конституция Республики Казахстан (принята на республиканском референдуме 15 марта 2026 г.) // https://prg.kz/document/?doc_id=35502996&pos=6;179

15. Уголовно-процессуальный кодекс Республики Казахстан: Кодекс от 4 июля 2014 года № 231-V // ИПС «Әділет». adilet.zan.kz/rus/docs/K1400000231.

РАМАЗАНОВ ДАУЛЕТ МУСТАФАЕВИЧ
Старший помощник ГП Республики Казахстан
Аппарата ГП Республики Казахстан,
Докторант Академии правоохранительных органов
при ГП Республики Казахстан
старший советник юстиции

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМ ОБЕСПЕЧЕНИИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ: ВОЗМОЖНОСТИ, РИСКИ И ПРАВОВЫЕ ГАРАНТИИ

Сегодня искусственный интеллект перестает быть исключительно технологической темой и становится фактором трансформации государственного управления, правоохранительной деятельности и системы противодействия преступности.

Для правоохранительных органов особое значение имеет не столько сама возможность применения искусственного интеллекта, сколько изменение характера информационно-аналитической работы. Современный сотрудник работает с массивами информации, объем которых постоянно увеличивается: материалы уголовных дел, оперативные сведения, финансовые операции, цифровые следы, документы, изображения, аудио- и видеоматериалы, сведения из открытых источников.

В этих условиях искусственный интеллект способен структурировать большие массивы данных, выявлять взаимосвязи, обнаруживать аномалии, классифицировать документы и формировать прогнозы.

Однако возникает принципиальный вопрос: где заканчивается аналитическая функция искусственного интеллекта и начинается юридически значимое решение человека?

На мой взгляд, именно этот вопрос должен находиться в центре научной дискуссии.

Цель доклада — показать, каким образом искусственный интеллект может использоваться в информационно-аналитическом обеспечении противодействия преступности, какие риски возникают при его применении и какие правовые гарантии необходимы для того, чтобы технологическое развитие не привело к ослаблению принципа законности и защиты прав человека.

Традиционная информационно-аналитическая модель выглядит следующим образом: сбор информации — обработка — анализ — подготовка аналитического материала — принятие решения.

Искусственный интеллект позволяет существенно изменить эту последовательность. Система может осуществлять предварительную структуризацию информации, выявлять статистические связи, находить повторяющиеся модели и формировать аналитические гипотезы.

Richard A. Berk в статье «Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement», опубликованной в Annual Review of Criminology в 2021 году, рассматривает возможности применения искусственного интеллекта и

прогнозной аналитики в правоохранительной деятельности и одновременно обращает внимание на вопросы точности, справедливости и прозрачности.

Отсюда следует первый принципиальный вывод: искусственный интеллект следует рассматривать не как замену сотрудника, а как инструмент интеллектуального усиления его аналитических возможностей.

Алгоритм способен обработать значительно больший объем информации, но не обладает самостоятельной юридической компетенцией. Он может выявить корреляцию, но корреляция не означает причинность. Он может определить вероятность события, но вероятность не означает установленный факт. Он может сформировать аналитическую гипотезу, но гипотеза не является доказательством.

Первое направление — анализ больших массивов данных. Алгоритмы могут использоваться для выявления взаимосвязей между лицами, организациями, событиями и финансовыми операциями, поиска аномалий и структурирования больших массивов документов.

Второе направление — прогнозирование преступности. В исследовании RAND Corporation «Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations» Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith и John S. Hollywood рассмотрели применение прогнозных методов в правоохранительной деятельности.

Третье направление — обработка естественного языка. ИИ может использоваться для анализа документов, извлечения информации, поиска совпадений, подготовки аналитических материалов и автоматической расшифровки аудиозаписей.

Четвертое направление — цифровая криминалистика. ИИ способен помогать анализировать изображения, видео, аудио и иные цифровые следы.

Во всех этих случаях необходимо различать обнаружение информации и ее юридическую оценку.

Особенно важно не переоценивать технологические возможности искусственного интеллекта.

Показательным является исследование Stefaniya Kozhevnikova, Denis Yukhnenko, Giulio Scola и Seena Fazel «Machine learning for violence prediction: A systematic review and critical appraisal», опубликованное в Journal of Criminal Justice в 2026 году, Volume 105, Article 102697, DOI 10.1016/j.jcrimjus.2026.102697.

Авторы исследовали 38 работ и 40 моделей машинного обучения для прогнозирования насильственного поведения. В 31 исследовании, то есть в 82% случаях, был выявлен высокий риск систематической ошибки. Диапазон AUC составил от 0,50 до 0,98.

Авторы также выявили проблемы переобучения, недостаточной прозрачности и низкой обобщаемости моделей и пришли к выводу, что существующие модели не могут быть рекомендованы для непосредственного внедрения без дальнейшего повышения их надежности и практической применимости.

Для правоохранительной практики это означает: высокая точность модели на исходном массиве данных еще не означает, что модель будет столь же надежна в

другой стране, регионе, временном периоде или системе правоохранительной деятельности.

Наиболее серьезная проблема может находиться не в алгоритме, а в исходных данных.

Rashida Richardson, Jason Schultz и Kate Crawford в работе «Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice», опубликованной в New York University Law Review в 2019 году, показали, что данные правоохранительных органов отражают не только реальную преступность, но и особенности самой практики выявления и регистрации правонарушений.

Если на определенной территории исторически осуществляется более интенсивный контроль, там может выявляться больше правонарушений. Алгоритм воспринимает статистику как признак повышенного риска. На основании прогноза туда направляются дополнительные ресурсы, что приводит к выявлению еще большего числа правонарушений.

Возникает алгоритмическая петля обратной связи.

Поэтому перед использованием данных необходимо оценивать их происхождение, полноту, репрезентативность, достоверность и наличие систематических искажений.

Andrew Guthrie Ferguson в книге «The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement», изданной NYU Press в 2017 году, исследует влияние больших данных и алгоритмического управления на правоохранительную деятельность.

Математическая форма результата сама по себе не делает его объективным. Если исходные данные содержат систематические искажения, алгоритм может их воспроизводить.

Вторая проблема — объяснимость. Если система сообщает сотруднику о высоком риске, сотрудник должен понимать, на чем основан такой вывод.

Joshua A. Kroll и соавторы в статье «Accountable Algorithms», опубликованной в University of Pennsylvania Law Review в 2017 году, обосновывают необходимость специальных механизмов алгоритмической подотчетности.

Для правоохранительной деятельности результат алгоритма должен быть проверяемым и документируемым: какая модель применялась, какие данные использовались, какова область применимости, когда проводилась валидация и каков уровень возможной ошибки.

Для Казахстана эта проблематика приобрела особую актуальность с принятием Закона Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте».

В официальной информационно-правовой системе «Әділет» Закон обозначен как обновленный; дата изменения — 24 июня 2026 года. Статья 4 закрепляет принципы законности, справедливости и равенства, прозрачности и объяснимости, ответственности и подконтрольности, приоритета благополучия человека и свободы его воли, защиты данных и конфиденциальности, безопасности и защищенности.

Для правоохранительной сферы особенно важны прозрачность, объяснимость, ответственность, подконтрольность и приоритет человека.

Закон предусматривает риск-ориентированный подход к системам ИИ. Следовательно, вопрос должен ставиться не только как «разрешить или запретить ИИ», а как определить допустимый уровень риска конкретной системы и соответствующие гарантии контроля.

Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности» определяет правовые основы соответствующей деятельности и устанавливает требования законности и соблюдения прав и свобод человека.

Отсюда следует принципиальное положение: искусственный интеллект не является самостоятельным основанием для проведения оперативно-розыскного мероприятия.

Алгоритм может выявить закономерность, предложить направление аналитической проверки или обратить внимание сотрудника на определенный массив данных. Но он не должен сам по себе расширять полномочия правоохранительного органа.

Предлагаемая формула: «Алгоритмический прогноз может инициировать аналитическую проверку, но не заменяет предусмотренное законом основание для ограничения прав человека».

Уголовно-процессуальный кодекс Республики Казахстан определяет процессуальные правила установления юридически значимых обстоятельств.

В этой сфере необходимо строго разграничивать аналитическую информацию, оперативную информацию, доказательственную информацию и процессуальное решение.

ИИ может обнаружить связь между объектами, выявить аномалию или сформировать прогноз. Но результат алгоритма не должен автоматически превращаться в доказательство.

Можно сформулировать границу следующим образом: ИИ может помочь найти факт, но не может самостоятельно придать ему юридическое значение; ИИ может сформировать версию, но не может самостоятельно установить виновность; ИИ может определить вероятность события, но вероятность не заменяет доказательство.

Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» устанавливает правовые основы сбора, обработки и защиты персональных данных.

Необходимо различать законность получения информации и законность ее последующего использования алгоритмом.

Особую проблему представляют публичные генеративные ИИ-сервисы. Передача в такие системы служебных документов, персональных данных или иной охраняемой информации может создавать риски утечки, неконтролируемого хранения и вторичного использования данных.

Для правоохранительной сферы более перспективным является создание защищенных ведомственных контуров обработки информации, в которых

контролируются доступ пользователей, хранение данных, журналирование действий и версия используемой модели.

Законодательство Казахстана также содержит специальные положения, связанные с автоматизированной обработкой персональных данных, включая ограничения, когда в результате такой обработки у субъекта возникают, изменяются или прекращаются права, кроме предусмотренных законом случаев.

В Европейском союзе действует Regulation (EU) 2024/1689 — Artificial Intelligence Act. В актуальной консолидированной версии от 27 июля 2026 года акт предусматривает риск-ориентированную систему регулирования и ограничения для ряда особо рискованных практик.

Особое значение для нашей темы имеет подход к predictive policing: регулирование проводит границу между использованием объективных и проверяемых фактов и определенными формами прогнозирования преступного поведения конкретных лиц, основанными исключительно на профилировании или характеристиках личности.

Совет Европы в 2024 году открыл для подписания Рамочную конвенцию об искусственном интеллекте и правах человека, демократии и верховенстве права.

ЮНЕСКО в Рекомендации по этике искусственного интеллекта 2021 года закрепляет ориентиры, связанные с человеческим достоинством, правами человека, прозрачностью, справедливостью и человеческим контролем.

NIST Artificial Intelligence Risk Management Framework 1.0 предлагает рассматривать управление рисками как непрерывный процесс на протяжении жизненного цикла ИИ-системы.

Общий вывод: современное регулирование движется не к полному отказу от ИИ, а к управляемому и контролируемому его применению.

Предлагается модель «пяти уровней правоохранительного ИИ».

Первый уровень — данные: происхождение, правомерность получения, качество, полнота, актуальность, репрезентативность и наличие систематических искажений.

Второй уровень — алгоритм: назначение модели, область допустимого применения, показатели эффективности, показатели ошибки, ограничения и результаты внешней валидации.

Третий уровень — аналитический результат: прогноз, классификация, выявленная взаимосвязь, обнаруженная аномалия или аналитическая рекомендация.

Четвертый уровень — профессиональная проверка: оценка качества результата, исходных данных, применимости модели, альтернативных объяснений и необходимости дополнительной проверки.

Пятый уровень — юридическое решение: только после профессиональной проверки принимается решение, имеющее юридическое значение.

На мой взгляд, именно эта последовательность может стать одним из принципов внедрения ИИ в правоохранительную деятельность Казахстана.

Следующим элементом должна стать система алгоритмического аудита. Аудит необходим до внедрения системы, после существенного изменения модели, периодически во время эксплуатации и после выявления существенной ошибки.

Проверяться должны качество данных, репрезентативность, алгоритмическая предвзятость, точность, калибровка, внешняя валидность, устойчивость результатов, объяснимость и информационная безопасность.

Не менее важен вопрос ответственности.

Нельзя допускать ситуацию, когда должностное лицо объясняет ошибочное решение словами: «Так показал искусственный интеллект».

ИИ не должен становиться способом размывания персональной ответственности.

Принцип должен быть простым: чем выше потенциальное воздействие ИИ на права человека, тем выше требования к валидации, объяснимости, аудиту и человеческому контролю.

Наиболее перспективным, на мой взгляд, является переход от вопроса «кто совершит преступление?» к вопросу «какие криминогенные процессы формируются и где требуется профилактическое вмешательство?»

ИИ может прогнозировать рост определенного вида преступности, территориальную концентрацию, временные пики, изменение структуры преступности, появление новых способов совершения преступлений и другие объективные факторы.

Такой подход позволяет использовать технологические преимущества ИИ и одновременно снижать риск персонализированной алгоритмической стигматизации.

В результате искусственный интеллект становится инструментом стратегической криминологической аналитики и может способствовать переходу от преимущественно реактивной модели к превентивной.

Но предупреждение о риске должно оставаться предупреждением о риске. Оно не должно превращаться в утверждение о наличии нарушения закона без предусмотренной законом проверки.

По итогам исследования предлагаю рассмотреть следующие меры.

Первое — разработать классификацию ИИ-систем по уровню воздействия на права и свободы человека.

Второе — установить обязательную оценку качества и происхождения данных до внедрения модели.

Третье — предусмотреть внешнюю валидацию моделей, используемых для индивидуальной оценки лиц.

Четвертое — ввести ведомственный алгоритмический аудит.

Пятое — создать реестр используемых правоохранительными органами систем ИИ.

Шестое — обеспечить обязательное журналирование алгоритмических результатов.

Седьмое — исключить использование одного лишь алгоритмического прогноза в качестве основания для вывода о виновности лица.

Восьмое — установить обязательный человеческий контроль за решениями, затрагивающими права и свободы человека.

Девятое — ограничить передачу служебной и иной охраняемой законом информации во внешние публичные генеративные ИИ-сервисы.

Десятое — подготовить сотрудников по вопросам алгоритмической грамотности.

Искусственный интеллект способен стать одним из ключевых инструментов трансформации информационно-аналитического обеспечения противодействия преступности.

Но его ценность определяется не степенью автономности, а способностью повышать качество профессиональной деятельности человека.

Научные данные 2026 года показывают, что существующие модели прогнозирования насильственного поведения пока имеют серьезные ограничения. В систематическом обзоре Kozhevnikova, Yukhnenko, Scola и Fazel только три из 38 исследований имели внешнюю валидацию, а в 31 исследовании был выявлен высокий риск систематической ошибки.

Следовательно, нельзя исходить из презумпции, что если решение принял алгоритм, оно объективнее.

Необходимо проверять данные, модель, результат и контекст его использования.

Казахстан уже создал базовую нормативную основу. Закон «Об искусственном интеллекте» закрепляет законность, справедливость, прозрачность, объяснимость, ответственность, подконтрольность, защиту данных, безопасность и приоритет человека.

Поэтому предлагаю в качестве основного принципа правоохранительного применения ИИ следующую формулу:

«Искусственный интеллект может формировать аналитическую гипотезу, но не должен самостоятельно формировать юридически значимое решение».

Организационно эту идею можно выразить пятью словами:

Данные. Алгоритм. Гипотеза. Человек. Закон.

Именно такая последовательность позволит использовать возможности искусственного интеллекта для повышения эффективности противодействия преступности, не отказываясь от фундаментального требования — приоритета закона и защиты прав человека.

Список использованных источников:

Нормативные правовые акты Республики Казахстан

1. Уголовно-процессуальный кодекс от 4 июля 2014 года № 231-V ЗРК.

2. Закон от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте».

3. Закон от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности».

4. Закон от 21 мая 2013 года № 94-V «О персональных данных и их защите».

Международные нормативные и рекомендательные документы

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down armonized rules on artificial intelligence (Artificial Intelligence Act). Consolidated version.

2. Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024.

3. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 23 November 2021.

4. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.AI.100-1.

Научная литература

1. Berk R. A. Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement // Annual Review of Criminology. 2021. Vol. 4. P. 209–237. DOI: 10.1146/annurev-criminol-051520-012342.

2. Kozhevnikova S., Yukhnenko D., Scola G., Fazel S. Machine learning for violence prediction: A systematic review and critical appraisal // Journal of Criminal Justice. 2026. Vol. 105. Article 102697. DOI: 10.1016/j.jcrimjus.2026.102697.

3. Richardson R., Schultz J., Crawford K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice // New York University Law Review. 2019. Vol. 94.

4. Ferguson A. G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: NYU Press, 2017.

5. Kroll J. A., Huey J., Barocas S., Felten E. W., Reidenberg J. R., Robinson D. G., Yu H. Accountable Algorithms // University of Pennsylvania Law Review. 2017. Vol. 165, No. 3.

6. Perry W. L., McInnis B., Price C. C., Smith S. C., Hollywood J. S. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica: RAND Corporation, 2013. RR-233-NIJ.

7. Europol Innovation Lab. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. The Hague, 2024.

8. The AI Act in a Law Enforcement Context: The Case of Automatic Speech Recognition for Transcribing Investigative Interviews // Forensic Science International: Synergy. 2024. Vol. 9. Article 100563.

САРСЕНБАЕВ ОЛЖАС АЗАРХАНОВИЧ
Докторант Академии правоохранительных органов
при ГП Республики Казахстан
магистр права и национальной безопасности
майор полиции

ПРЕЗУМПЦИЯ НЕВИНОВНОСТИ В УСЛОВИЯХ ОБЩЕСТВЕННОГО СУБЪЕКТИВИЗМА И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ

Аннотация. *В статье рассматриваются особенности реализации принципа презумпции невиновности в уголовном судопроизводстве Республики Казахстан в условиях усиления общественного субъективизма, медиавлияния и развития искусственного интеллекта. Раскрывается понятие общественного субъективизма как социально-правового феномена, при котором массовые оценки, эмоции и стереотипы способны подменять объективную юридическую оценку обстоятельств уголовного дела. Анализируются противоречия между нормативным закреплением презумпции невиновности и рисками её формальной реализации, включая обвинительный уклон и преждевременную криминализацию личности в информационном пространстве. Особое внимание уделено двойственной роли искусственного интеллекта: возможности аналитической поддержки правоохранительной деятельности и риску воспроизводства алгоритмической предвзятости. Предлагается концепция интеллектуального мониторинга медиапространства для выявления признаков общественного давления без определения виновности конкретного лица. Обосновывается необходимость прозрачности алгоритмов, защиты персональных данных, недискриминации и обязательного человеческого контроля.*

Ключевые слова: *презумпция невиновности, общественный субъективизм, искусственный интеллект, уголовный процесс, медиавлияние, обвинительный уклон, алгоритмическая предвзятость, цифровизация, человеческий контроль.*

Введение. Принцип презумпции невиновности закреплён в статье 19 Уголовно-процессуального кодекса Республики Казахстан (далее — УПК РК). В соответствии с ним бремя доказывания обвинения возлагается на сторону обвинения, а неустранимые сомнения в виновности толкуются в пользу обвиняемого [1]. Данный принцип исключает подмену доказательственной оценки личным отношением к подозреваемому или обвиняемому и предполагает установление виновности в предусмотренном законом порядке [2].

В условиях цифровизации общественное мнение приобретает дополнительное влияние на восприятие уголовно-правовых конфликтов. Средства массовой информации и социальные сети способны формировать устойчивые оценки ещё до завершения расследования и судебного разбирательства. Стремление к быстрому и демонстративному наказанию создаёт риск, при котором общественное убеждение начинает восприниматься как подтверждение

виновности, хотя оно не обладает самостоятельным доказательственным значением [3].

Актуальность исследования обусловлена противоречием между формальным закреплением презумпции невиновности и социальными механизмами, способными ослаблять её практическое действие. Дополнительный аспект проблемы связан с искусственным интеллектом, который может как способствовать анализу информационной среды, так и воспроизводить существующие предубеждения.

Цель исследования – раскрыть влияние общественного субъективизма на реализацию презумпции невиновности и определить возможности использования искусственного интеллекта для выявления рисков общественного давления при сохранении процессуальных гарантий личности.

Материалы и методы. Исследование основано на анализе нормативных правовых актов Республики Казахстан, международных документов и научных трудов отечественных и зарубежных авторов. Применены диалектический, исторический, сравнительно-правовой и формально-юридический методы, а также методы аналитической философии права и юридической герменевтики.

Основная часть. Презумпция невиновности закреплена не только статьёй 19 УПК РК, но и статьёй 77 Конституции Республики Казахстан. Её содержание соответствует международным стандартам защиты прав человека, включая положения Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах [4]. Данный принцип выступает гарантией того, что вывод о виновности не может основываться исключительно на предположениях, общественном осуждении или предварительной версии расследования.

Несмотря на нормативное закрепление, сохраняется проблема реального действия презумпции невиновности в условиях общественного субъективизма. Для раскрытия данного явления необходимо разграничить объективную юридическую оценку и общественные представления о виновности.

Понятие «общественный» указывает на массовые, групповые или доминирующие представления, распространяющиеся посредством СМИ, социальных сетей, публичных дискуссий и иных каналов коммуникации [5]. Такие представления не обладают юридической обязательностью, однако могут формировать общественные ожидания и фактически воздействовать на участников уголовного процесса [6].

Субъективизм связан с преобладанием субъективного фактора над объективными закономерностями и обстоятельствами. В научном познании он проявляется в игнорировании или недооценке объективных факторов под влиянием личных либо групповых убеждений [7; 8]. Применительно к уголовному судопроизводству подобный подход выражается в формировании выводов о виновности на основании эмоций, стереотипов, фрагментарной информации и предварительных оценок, а не проверенных доказательств.

На основе проведённого анализа предлагается следующее авторское определение:

Общественный субъективизм – это социально обусловленный феномен, выражающийся в совокупности массовых, групповых или доминирующих оценочных представлений, формирующихся в общественном сознании в процессе социальной коммуникации и основанных преимущественно на игнорировании или недооценке значимости объективных факторов и закономерностей, доказательств и правовых стандартов.

Опасность данного феномена заключается в том, что общественная оценка способна опережать юридическую процедуру и формировать устойчивое убеждение в виновности лица до вынесения судебного решения. При этом общественное мнение не заменяет доказательства и не освобождает органы уголовного преследования от обязанности соблюдать установленные законом процессуальные требования.

Теоретическое осмысление данной проблемы связано с соотношением рационального и иррационального в праве. В. В. Хан подчёркивает значение рациональных правовых ориентиров и необходимость их сохранения при воздействии деформированных форм правосознания [9].

Рациональное начало уголовного процесса выражается в общеобязательных правовых критериях, обеспечивающих защиту прав и свобод человека. Иррациональное проявляется в ситуациях, когда эмоции, стереотипы и субъективные ожидания начинают преобладать над установленными процедурами и объективной оценкой обстоятельств. В результате право рискует утратить свою гарантийную функцию, а презумпция невиновности – превратиться в формальное положение.

Таким образом, общественный субъективизм следует рассматривать как самостоятельную аналитическую категорию, позволяющую объяснить противоречие между рациональной природой уголовно-процессуального права и иррациональными механизмами массового восприятия.

Одной из проблем реализации презумпции невиновности является возможный разрыв между её нормативным закреплением и фактической правоприменительной практикой. Если первоначально выдвинутая версия обвинения воспринимается как практически предопределённый результат, расследование рискует превратиться в поиск подтверждений этой версии вместо всестороннего исследования обстоятельств дела.

Низкая доля оправдательных приговоров и преобладание обвинительных решений могут интерпретироваться по-разному: как результат эффективности системы правосудия либо как возможное проявление устойчивого обвинительного уклона. Поэтому статистические показатели сами по себе не позволяют однозначно установить наличие такого уклона, но служат основанием для постановки вопроса о полноте проверки доказательств и альтернативных версий [10].

Особое значение имеет первоначальная оценка события. Если версия виновности приобретает определяющее значение на раннем этапе, последующие процессуальные действия могут преимущественно ориентироваться на подтверждение уже сформированного вывода. В подобных условиях оправдывающие обстоятельства рискуют получить недостаточное внимание.

Как отмечает В. В. Хан, проблема презумпции невиновности связана и с теоретическими особенностями уголовного процесса, в котором наличие обвинения способно заранее определять направление процессуальной деятельности [11].

Следовательно, практическая реализация презумпции невиновности требует не только формального соблюдения процессуальных норм, но и объективного исследования как уличающих, так и оправдывающих обстоятельств. Обвинительная версия должна оставаться проверяемым предположением, а не предопределённым результатом расследования.

Расширение информационного пространства усиливает значение публичных сообщений при формировании общественного отношения к уголовным делам. Скорость распространения информации, многократное воспроизведение публикаций и эмоциональная подача событий могут способствовать закреплению обвинительных оценок ещё до завершения судебного разбирательства.

Преждевременное обозначение подозреваемого или обвиняемого как преступника способно негативно повлиять на его репутацию и сформировать общественное убеждение в виновности. Подобная практика создаёт риски для справедливого судебного разбирательства и защиты чести, достоинства и деловой репутации личности [12].

При этом нарушение презумпции невиновности не следует автоматически отождествлять с клеветой. Для юридической квалификации распространённых сведений необходимо установить соответствующие предусмотренные законом признаки. Некорректное освещение уголовного дела может быть связано не только с намеренным распространением ложной информации, но и с поспешными выводами, неточными формулировками или недостаточным разграничением фактов и оценок.

Законодательство предусматривает механизмы защиты нарушенных прав, включая опровержение недостоверных сведений и возмещение причинённого вреда [13]. Вместе с тем обеспечение презумпции невиновности не предполагает полного ограничения общественной дискуссии или свободы выражения мнения.

Необходимым условием является разграничение установленных фактов, сведений о процессуальном статусе лица и оценочных суждений. Общественное обсуждение уголовного дела допустимо, однако оно не должно подменять судебное установление виновности.

Искусственный интеллект расширяет возможности правоохранительной деятельности благодаря обработке значительных массивов информации, выявлению закономерностей и сопоставлению разрозненных данных. Вместе с тем применение таких технологий в уголовной юстиции затрагивает права личности и поэтому не может оцениваться исключительно с позиции технологической эффективности.

Основной риск заключается в возможности алгоритмической предвзятости. Если данные, используемые для обучения системы, содержат устойчивые стереотипы или обвинительные установки, алгоритм может воспроизводить их в результатах анализа. Дополнительную опасность представляют непрозрачность алгоритмических решений, ошибочная классификация информации и автоматизированное усиление эмоционально насыщенного контента.

Таким образом, цифровизация сама по себе не гарантирует объективности. Искусственный интеллект способен снижать отдельные проявления человеческого субъективизма, но при ненадлежащей организации может воспроизводить его в алгоритмической форме.

Международные подходы к применению ИИ в судебных системах подчёркивают значение соблюдения фундаментальных прав, недискриминации, прозрачности, качества, беспристрастности и контроля со стороны человека. Эти ориентиры отражены в Европейской этической хартии CEPEJ [14].

Аналогичные требования имеют значение для Республики Казахстан. Законодательство об искусственном интеллекте закрепляет принципы законности, справедливости, прозрачности и объяснимости, ответственности и подконтрольности, защиты данных и безопасности [15]. В уголовной юстиции соблюдение этих принципов особенно важно, поскольку ошибочный алгоритмический результат может затронуть конституционные права человека.

В связи с этим искусственный интеллект следует рассматривать как вспомогательный аналитический инструмент, а не как самостоятельного субъекта принятия процессуальных решений. Он не должен заменять оценку доказательств следователем, прокурором или судом, а его выводы не могут автоматически рассматриваться как подтверждение виновности.

В качестве перспективного направления предлагается разработка системы интеллектуального мониторинга общественного субъективизма, предназначенной для выявления признаков информационного давления вокруг уголовных дел.

Система могла бы использовать методы обработки естественного языка и машинного обучения для анализа открытого информационного пространства. В частности, возможно формирование условного индекса информационного давления на основе следующих показателей: соотношение фактических сообщений и оценочных суждений, частота употребления обвинительных формулировок, динамика распространения и повторяемость публикаций, случаи подмены процессуального статуса лица утверждением о его виновности, концентрация обвинительных сообщений вокруг конкретного уголовного дела.

Указанные показатели являются предлагаемыми аналитическими критериями, а не уже апробированной методикой. Их практическое применение потребует определения измеримых параметров, проверки точности классификации и оценки возможных ошибок.

Принципиально важно, чтобы индекс информационного давления не использовался для установления виновности конкретного лица и не приобретал значения доказательства по уголовному делу. Его назначение должно ограничиваться выявлением потенциальных рисков общественного давления и формированием сигнала о необходимости повышенного внимания к соблюдению процессуальных гарантий.

Предлагаемый подход предполагает разграничение двух направлений использования ИИ. Первое связано с аналитической поддержкой противодействия преступности, включая выявление закономерностей и обработку информационных массивов. Второе имеет превентивно-правозащитный характер и направлено на

выявление информационных факторов, способных создавать угрозу объективному рассмотрению уголовного дела.

Результатом мониторинга во втором случае должно становиться не определение виновности, а фиксация наблюдаемых признаков информационного давления. При этом необходимо обеспечить прозрачность критериев анализа, защиту персональных данных, возможность проверки результатов и обязательный человеческий контроль.

Таким образом, интеллектуальный мониторинг может рассматриваться как инструмент раннего выявления рисков для презумпции невиновности. Его ценность заключается в способности обратить внимание на расхождение между общественной оценкой и юридической процедурой, не вмешиваясь в компетенцию органов, уполномоченных принимать процессуальные решения.

Заключение. Проведённое исследование позволяет сделать вывод о том, что реализация презумпции невиновности в современных условиях сталкивается с вызовами, связанными с общественным субъективизмом, медиавлиянием и развитием искусственного интеллекта.

Предложенное определение общественного субъективизма позволяет раскрыть механизм, посредством которого массовые оценки, эмоции и стереотипы способны подменять объективную юридическую оценку и оказывать фактическое давление на участников уголовного процесса. При этом общественное мнение не обладает самостоятельным доказательственным значением и не может заменять предусмотренную законом процедуру установления виновности.

Обвинительный уклон и преждевременная криминализация личности создают риск формального восприятия презумпции невиновности. Для укрепления данного принципа необходимо обеспечивать объективное исследование всех обстоятельств дела, включая оправдывающие, а также разграничивать установленные факты и оценочные суждения в публичном информационном пространстве.

В качестве перспективного направления предложена концепция интеллектуального мониторинга общественного субъективизма, позволяющая выявлять признаки информационного давления вокруг уголовных дел. При этом искусственный интеллект должен выполнять исключительно вспомогательную функцию. Его результаты не могут подменять оценку доказательств и принятие процессуальных решений уполномоченным человеком.

Следовательно, эффективное использование цифровых технологий в уголовной юстиции возможно лишь при соблюдении принципов законности, прозрачности, объяснимости, защиты данных, недискриминации и обязательного человеческого контроля. Только при таком подходе технологическое развитие может способствовать защите презумпции невиновности, не ослабляя фундаментальные гарантии прав личности.

Список литературы:

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК (ред. от 16.09.2025) // Интернет-ресурс: https://adilet.zan.kz/rus/docs/K1400000231 дата обращения напр.: 20.12.2025 г.

2. Канкулов А.Х. Принцип презумпции невиновности как основа уголовного судопроизводства // Право и государство: теория и практика. – 2021. – № 8 (200). – С. 93-94.

3. Токсанова М.Б. Влияние общественного мнения на эффективность управления правоохранительными органами // Вестник науки. – 2025. – Т. 2. – № 3 (84). – С. 238-244.

4. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (ред. от 01.01.2023) // Интернет-ресурс: https://adilet.zan.kz/rus/docs/K950001000_ дата обращения напр.: 20.12.2025 г.

5. Мухамадиева Г.Н. Некоторые проблемы реализации принципа презумпции невиновности в уголовном процессе // Вестник КазНУ. Серия юридическая. – 2015. – № 1 (73). – С. 380-385.

6. Шавеко Н.А. Общественное мнение и справедливость // Право: история и современность. – 2022. – № 1 (6). – С. 35-45.

7. Коварж Г.Ю. Объективизм и субъективизм в научном познании // Социум – Наука – Инновации: сб. статей Всерос. научно-практич. конф. с международ. участием. – Уфа: Аэтерна, 2023. – С. 114-117.

8. Ефимов В.И. Ошибки, заблуждения, ложь, обман: монография. – М., 2014. – 255 с.

9. Хан В.В. Дихотомия «иррациональное/рациональное» как теория познания принципов уголовного процесса // Ученые труды Алматинской академии МВД РК им. М. Есбулатова. – 2022. – № 4 (73). – С. 367-375.

10. Правовая статистика // Интернет-ресурс: https://qamqor.gov.kz/crimestat/statistics дата обращения напр.: 20.12.2025 г.

11. Хан В.В. Презумпция невиновности как коррелят материальной истины // Вестник Академии правоохранительных органов. – 2025. – № 1 (35). – С. 203-209.

12. Гусакова В.Г., Часовникова О.Г. Презумпция невиновности в контексте современного медиапространства // Научный Лидер. – 2025. – № 20 (221). – С. 136-138.

13. Закон Республики Казахстан «О масс-медиа» от 19 июня 2024 года № 93-VIII ЗРК (ред. от 17.11.2025) // Интернет-ресурс: https://adilet.zan.kz/rus/docs/Z2400000093 дата обращения напр.: 20.12.2025 г.

14. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Council of Europe, 2018.

15. Закон Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК (ред. от 25.08.2026) // Информационно-правовая система «Әділет».

СЫСОЕВ АЛЕКСЕЙ СЕРГЕЕВИЧ
Начальник кафедры оперативно-розыскной деятельности факультета милиции Учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» полковник милиции

ВОЗМОЖНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПОДГОТОВКЕ И ПРОВЕДЕНИИ УЧЕБНЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ «ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ»

В последние десятилетия искусственный интеллект стал неотъемлемой частью повседневной жизни, найдя активное применение и в социальной сфере. Одной из самых перспективных областей применения искусственного интеллекта является образование. В условиях быстро меняющегося мира, где знания и навыки становятся ключевыми факторами успеха, необходимость внедрения возможностей искусственного интеллекта в образовательный процесс видится особенно актуальной.

Рассмотрим возможности применения искусственного интеллекта в образовательном процессе на примере подготовки и проведения лекционного занятия по дисциплине «Оперативно-розыскная деятельность органов внутренних дел». Материалы к лекционному занятию готовились по открытым источникам, основу которых составляют положения Закона Республики Беларусь «Об оперативно-розыскной деятельности» от 15 июля 2015 г. № 307-З (далее – Закон).

Целью лекционного занятия являлось сравнение подготовленных преподавателем на основе анализа норм Закона материалов по вопросу: «Основания и общие условия проведения оперативно-розыскных мероприятий вне рамок дел оперативного учёта» с материалами, разработанными наиболее популярными нейросетями QWEN и Deep Seek.

Так, по решению должностного лица органа, осуществляющего оперативно-розыскную деятельность, без вынесения постановления, проводятся следующие оперативно-розыскные мероприятия:

- Оперативный опрос (статья 21 Закона).
- Оперативное отождествление (статья 25 Закона).
- Оперативный осмотр (статья 26 Закона). Исключение составляют осмотр в виде обследования жилища и иного законного владения гражданина, помещения, здания, сооружения, транспортного средства, иного объекта и территории организации, проводимый негласно и связанный с проникновением в (на) них в отсутствие собственника, а также в виде изучения информационных систем, информационных ресурсов, предметов и документов, компьютерной информации, содержащих сведения, составляющие банковскую, врачебную, коммерческую и иную охраняемую законом тайну.
- Наблюдение в общественных местах, на участках местности, а также во всех видах общественного транспорта (статья 27 Закона), за исключением наблюдения

с использованием средств негласного получения (фиксации) информации и иных средств, установленных в жилище и ином законном владении гражданина, помещении, здании, сооружении, транспортном средстве, на ином объекте и территории организации.

- Сбор образцов (статья 23 Закона).

Также при наличии оснований, вне рамок дела оперативного учёта могут проводиться оперативно-розыскные мероприятия наведение справок (статья 22 Закона) и исследование предметов и документов, компьютерной информации (статья 24 Закона).

В свою очередь часть 6 статьи 19 Закона содержит исчерпывающий перечень оперативно-розыскных мероприятий, проводимых только в рамках дел оперативного учёта, а именно: проверочная закупка, контролируемая поставка, слуховой контроль, контроль в сетях электросвязи, контроль почтовых отправлений, оперативное внедрение и оперативный эксперимент.

Однако, из вышеуказанной нормы есть исключение, также прописанное в часть 6 статьи 19 Закона и указывающее, что оперативно-розыскные мероприятия, проводимые по основаниям, предусмотренным абзацами 4, 10, 12 и 14 части 1 статьи 16, могут проводиться вне рамок дел оперативного учета:

- абзац 4: поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении;

- абзац 10: письменный запрос органа, осуществляющего оперативно-розыскную деятельность, о проведении оперативно-розыскного мероприятия по основаниям, указанным в абзацах втором–девятом настоящей части;

- абзац 12: письменный запрос международной организации, правоохранительного органа, специальной службы иностранного государства в соответствии с международными договорами Республики Беларусь, а также на основе принципа взаимности;

- абзац 14: необходимость сбора сведений для принятия решений о допуске граждан к государственным секретам, к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья граждан и окружающей среды, к участию в оперативно-розыскной деятельности, к содействию на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность.

Подготовленный нейросетью QWEN материал, в целом, можно использовать при подготовке к лекционному занятию, однако он требовал корректировки, по причине допущенных нейросетью ошибок, связанных с неправильным толкованием некоторых норм Закона.

Так, нейросеть указала лишь 5 из 7 оперативно-розыскных мероприятий, проведение которых возможно без заведения дела оперативного учёта.

Кроме этого, QWEN ошибочно ссылается на часть 9 статьи 17 Закона, предоставляющую возможность проведения оперативно розыскных мероприятий по абзацам 4, 10, 12 и 14 части 1 статьи 16 Закона вне рамок дел оперативного учета. Данные условия указаны в части 9 статьи 19 Закона.

Кроме этого, QWEN не разграничила возможность проведения таких оперативно-розыскных мероприятий как оперативный осмотр и наблюдение, указав, что они проводятся только в рамках дел оперативного учета при необходимости получения санкции прокурора, что не соответствует действительности по изложенным выше причинам.

Проведённый нейросетью DEEP SEEK анализ также требует тщательной проверки и устранения ряда недостатков.

Ссылаясь на статью 17 Закона DEEP SEEK указывает, что дела оперативного учёта заводятся при наличии оснований, предусмотренных пунктами 1–6, 8, 10 и 11 части 1 статьи 16 Закона. Однако, при толковании Закона используются термины статья и абзац.

Кроме этого, абзац 1 части 1 статьи 17 дела предусматривает заведение дела оперативного учёта при наличии одного из оснований для проведения оперативно-розыскного мероприятия, предусмотренного абзацами 2, 5–9 части 1 статьи 16 Закона.

Также DEEP SEEK неверно указывает основание для проведения оперативно-розыскных мероприятий без заведения дела оперативного учёта – необходимость сбора сведений для принятия решений о применении мер по обеспечению безопасности граждан, оказывающих или оказывавших содействие на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность (абзац 13 ч. 1 ст. 16 Закона).

Абсолютно неверно нейросетью указываются основания к проведению оперативно-розыскных мероприятий без заведения дела оперативного учёта в связи с розыском отдельных категорий граждан абзацы 7, 8 и 9 части 1 статьи 16 Закона (без вести пропавшие, погибшие (умершие) персональные данные которых не установлены и граждане, которые в силу состояния здоровья или возраста не могут сообщить о себе сведения).

Последнее заблуждение связано с отсутствием у нейросети практического опыта применения Закона, подтверждением чему служит следующий пример.

Так, при поступлении в орган внутренних дел заявления или сообщения о безвестном исчезновении гражданина и последующему возбуждению уголовного дела по данному факту, предшествует доследственная проверка. В соответствии с требованиями Уголовно-процессуального кодекса Республики Беларусь (далее – УПК), срок проведения проверки составляет 10 суток, и при наличии определённых условий, может быть продлён прокурором до одного месяца (часть 1 статьи 173).

Во время проверки в порядке УПК, оперативный сотрудник вправе проводить все предусмотренные Законом оперативно-розыскные мероприятия, при условии, что начальником органа внутренних дел или лицом, временно исполняющим его обязанности, дано соответствующее указание. Исходя из вышеизложенного, основанием для проведения оперативно-розыскных мероприятий при проведении проверки по факту безвестного исчезновения лица будет являться абзац 4 части 1 статьи 16 Закона (поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении).

Таким образом, указанное нейросетью DEEP SEEK основание проведения оперативно-розыскных мероприятий для установления местонахождения без вести пропавшего лица (абзац 7 ч. 1 статьи 16 Закона) будет законно лишь при наличии дела оперативного учёта. При этом, основанием к заведению дела оперативного учёта послужит возбуждение уголовного дела о безвестном исчезновении лица и предоставление в орган внутренних дел копии процессуального документа, подтверждающего принятие такого решения.

Подводя итог, можно отметить, что возможности искусственного интеллекта, а именно нейросетей QWEN и DEEP SEEK можно использовать при подготовке дидактического материала к учебным занятиям, однако информация, которую ненейросеть интегрирует из Интернета, требует тщательного анализа и проверки, о чём свидетельствуют приведённые выше примеры.

Список литературы:

1. Об оперативно-розыскной деятельности : Закон Респ. Беларусь от 15 июля 2015 г. № 307-З : в ред. от 07 фев. 2023 г. № 248-З // ЭТАЛОН : информ.-поисковая система (дата обращения 23.08.2026).

2. Уголовно-процессуальный кодекс Республики Беларусь: принят Палатой представителей 24 июня 1999 г.: обдобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 20 июля 2026 г. № 173-З // ЭТАЛОН : информ.-поисковая система (дата обращения 23.08.2026).

ХАКИМОВ ЕРЖАН МАРАТОВИЧ
Заместитель начальника Научно-исследовательского института Академии управления МВД Республики Казахстан доктор философии (PhD), ассоциированный профессор (доцент)

ЖУБАНДЫКОВА ЛЯЗЗАТ АБИЛКАИРОВНА
Старший научный сотрудник Центра по исследованию проблем управления ОВД Научно-исследовательского института Академии управления МВД Республики Казахстан доктор философии (PhD)

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРЕДПУБЛИКАЦИОННОЙ ПРОВЕРКЕ ОФИЦИАЛЬНЫХ СООБЩЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ: ПРАВОВАЯ МОДЕЛЬ И ПРЕДЕЛЫ АВТОМАТИЗАЦИИ

Введение

В Послании Главы государства от 8 сентября 2025 г. «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» поставлена задача превращения Казахстана в течение трех лет в полноценную цифровую страну и указано на необходимость выстроить интеллектуальную систему противодействия киберпреступности [1]. Указом Президента Республики Казахстан от 6 января 2026 г. № 1151 «в целях дальнейшего развития цифровизации и повсеместного внедрения искусственного интеллекта» 2026 год объявлен Годом цифровизации и искусственного интеллекта [2]. За короткий срок сформирована нормативная база: вступил в силу Закон Республики Казахстан «Об искусственном интеллекте» [3], принят Цифровой кодекс Республики Казахстан [4], Закон «Об информатизации» в связи с принятием Кодекса переработан в Закон «О кибербезопасности» [5]. Для органов внутренних дел это означает обязанность встраивать технологии искусственного интеллекта (далее – ИИ) в служебную деятельность с соблюдением прав граждан и принципа человекоцентричности, на котором делает акцент Послание [1].

Отечественная наука рассматривает ИИ в правоохранительной сфере преимущественно применительно к уголовному судопроизводству. Н.В. Сидорова и А.М. Серикбаев предлагают автоматизированное рабочее место следователя, которое указывает на аномальные процессуальные решения, и рекомендуют ориентироваться на принципы Европейской этической хартии [6]. А.А. Салимгерей и соавторы анализируют проблемы реализации Закона «Об искусственном интеллекте» и уровень грамотности населения в этой сфере [7], Н. Саулен и соавторы обосновывают роль ИИ как дополнения, а не замены человека в законотворчестве [8]. Наиболее близкую к нашей задачу решает Э.В. Талапина, рассматривающая ИИ как помощника при правовой экспертизе текстов в государственном управлении при сохранении итогового решения и подписи за ответственным служащим [9]. В зарубежной литературе подробно исследованы риски алгоритмической предвзятости и подотчетности полицейских алгоритмов

[10; 11], а INTERPOL и UNICRI разработали инструментарий ответственного внедрения ИИ в правоохранительных органах [12]. Однако официальная коммуникация полиции как сфера применения ИИ в этих работах не рассматривается.

Между тем именно здесь ошибка становится публичной мгновенно и необратимо. Сообщение, в котором задержанный назван «виновным лицом», опубликована фотография подозреваемого или по сочетанию признаков узнаваем ребенок, тиражируется средствами массовой информации и уже не может быть отозвано. Ранее проведенный авторами анализ пятнадцати эпизодов официальной коммуникации органов внутренних дел за 2025-2026 гг. показал, что такие нарушения повторяются и относятся к ограниченному числу типов, а значит, могут проверяться автоматизированно.

Цель исследования – обосновать правовую модель применения ИИ-ассистента для предпубликационной проверки официальных сообщений органов внутренних дел и определить пределы автоматизации такой проверки.

Материалы и методы

Нормативную базу составили Закон «Об искусственном интеллекте» [3], Цифровой кодекс [4], законы «О кибербезопасности» [5], «О персональных данных и их защите» [13], «О доступе к информации» [14] и Уголовно-процессуальный кодекс Республики Казахстан [15]. Сравнительный материал включает замечание общего порядка № 25 Комитета ООН по правам ребенка [16], Регламент (ЕС) 2024/1689 об искусственном интеллекте [17], Директиву (ЕС) 2016/343 о презумпции невиновности [18], рекомендации Всемирной организации здравоохранения для работников СМИ [19] и Европейскую этическую хартию об использовании ИИ в судебных системах [20].

Эмпирическую базу образуют пятнадцать эпизодов официальной коммуникации органов внутренних дел: семь эпизодов 2026 г. с участием несовершеннолетних (Н-1 – Н-7) и восемь эпизодов 2025-2026 гг., связанных с резонансными происшествиями (Р-1 – Р-8), ранее закодированных авторами по единым критериям. Источниками послужили официальный медиапортал МВД и публикации СМИ, воспроизводящие официальные сообщения.

Требования законодательства и международных стандартов к содержанию сообщений переведены в проверяемые правила (метод формализации). Каждое правило отнесено к одному из трех типов: детерминированное (проверка по словарю, шаблону или наличию элемента), вероятностное (классификация текста языковой моделью с выдачей предупреждения) и экспертное (оценка контекста, недоступная для надежной автоматизации). Затем проведено экспертное моделирование: для каждого выявленного ранее нарушения определено, каким правилом и каким типом проверки оно было бы обнаружено. Моделирование носит аналитический характер и не является испытанием программного продукта; его результаты задают требования к будущей системе.

Результаты

Правовые рамки ИИ-ассистента. Закон «Об искусственном интеллекте» закрепляет приоритет человека как ключевой принцип: применение ИИ не должно ограничивать возможность принимать осознанные решения, а участники

жизненного цикла системы обязаны сохранять постоянный контроль над ее функционированием [3]. Следовательно, ассистент может только предупреждать и предлагать исправления; решение о публикации принимает должностное лицо. Закон также запрещает системы, использующие уязвимость лица по признаку возраста, и системы, нарушающие законодательство о персональных данных [3]: ассистент, назначение которого – защищать персональные данные и права несовершеннолетних, этим целям соответствует, но сам должен быть построен с их соблюдением.

Цифровой кодекс требует, чтобы алгоритмические и автоматизированные решения, затрагивающие права человека, отвечали требованиям прозрачности и недискриминации, а субъект данных вправе получить понятное объяснение и требовать рассмотрения решения человеком [4]. Предупреждение ассистента не является решением о правах лица, но эти положения задают ориентир: каждое срабатывание должно сопровождаться указанием правила и фрагмента текста. Кодекс также содержит нормы об электронной цифровой подписи, ранее закрепленные в Законе «Об электронном документе и электронной цифровой подписи» [4]; подписание итогового текста ЭЦП ответственного должностного лица фиксирует, что окончательное решение принято человеком.

Проект официального сообщения содержит сведения досудебного расследования, которые могут быть преданы огласке лишь в допустимом объеме [15], и персональные данные, распространение которых ограничено законом [13]. Поэтому передача таких текстов во внешние общедоступные сервисы генеративного ИИ недопустима: ассистент должен функционировать в защищенном ведомственном контуре с соблюдением требований Закона «О кибербезопасности» [5]. Наконец, Закон «О доступе к информации» обязывает государственный орган информировать общество о своей деятельности [14]. Отсюда требование, которое часто упускается: ассистент должен проверять не только избыточность, но и полноту сообщения, иначе он станет инструментом информационного вакуума.

Правила проверки. На основе требований презумпции невиновности [15; 18], законодательства о персональных данных [13], стандартов защиты детей [16] и рекомендаций ВОЗ [19] сформулированы десять правил (таблица 1).

Таблица 1 – Правила предпубликационной проверки официальных сообщений

№Правило		Что проверяет ассистент	Тип проверки	Эпизоды
1	Презумпция невиновности	Формулы «виновное лицо», «преступник», «понесет наказание по всей строгости» рядом с указанием на конкретного задержанного	Детерминированная	Р-2
2	Персональные данные и изображение	Фамилия, имя, полная дата рождения, фотография или видео с лицом подозреваемого, правонарушителя, ребенка	Детерминированная	Р-2, Р-4
3	Правило трех признаков	Одновременное наличие точного возраста, малого населенного пункта или учебного заведения и специфических обстоятельств	Вероятностная (выделение признаков автоматически,	Н-2, Н-5

			оценка – человеком)	
4	Сведения о поведении и прошлом лица	Переписка, поведение потерпевшего, прежние правонарушения подозреваемого до решения суда	Вероятностная	Н-1, Р-6
5	Кризисные ситуации	Указание места, этажа, способа, видеозапись момента кризиса; наличие телефона доверия 150	Детерминированная	Н-7
6	Узнаваемое описание	Описание лица по роду занятий, известности, местным приметам	Экспертная	Р-5
7	Полнота сообщения	Наличие факта события, принятых мер, статьи закона, процессуального статуса	Детерминированная	Р-7
8	Жизненный цикл публикации	Связь сообщения об обнаружении ребенка с ранее опубликованным розыском; задание на обновление	Детерминированная	Н-3
9	Опровержение без устрашения	Соединение опровержения слуха со ссылкой на уголовную ответственность за распространение ложной информации	Детерминированная	Р-3
10	Своевременность	Наличие в публичном пространстве версии о причастности сотрудников при отсутствии официальной реакции	Экспертная (вне проверки текста)	Р-1

Источник: составлено авторами.

Результаты моделирования. В пятнадцати эпизодах ранее было выявлено тринадцать нарушений; эпизоды Н-4, Н-6 и Р-8 нарушений не содержали и служат контрольными – ассистент не должен выдавать по ним ложных предупреждений. Семь нарушений (Н-3, Н-7, два нарушения в Р-2, Р-3, Р-4, Р-7) обнаруживаются детерминированными правилами: оценочная лексика, фотография и полные персональные данные, отсутствие источников помощи в сообщении о кризисной ситуации, отсутствие квалификации деяния, неактуализированная публикация о розыске, соединение опровержения с напоминанием об уголовной ответственности. Четыре нарушения (Н-1, Н-2, Н-5, Р-6) выявляются лишь в форме предупреждения, требующего оценки человеком: раскрытие сведений о поведении и прошлом лица и косвенная идентификация ребенка. Два нарушения (Р-1, Р-5) находятся за пределами возможностей проверки текста: запоздалая реакция на сложившуюся в обществе версию и узнаваемое описание лица, понятное только жителям конкретного города.

Существенно, что наиболее тяжелые по последствиям нарушения – косвенная идентификация ребенка и запаздывание официальной позиции – автоматизируются хуже всего. Ассистент надежно устраняет грубые ошибки, но не заменяет профессиональную оценку контекста.

Обсуждение

Полученные результаты определяют место ИИ в официальной коммуникации полиции как «второго читателя», а не автора и не цензора. Такой подход согласуется с принципом приоритета человека [3], с моделью ИИ-помощника в правовой экспертизе, предложенной Э.В. Талапиной [9], и с инструментарием INTERPOL и UNICRI, который связывает ответственное внедрение ИИ в правоохранительных

органах с соблюдением прав человека и этических принципов [12]. По классификации Регламента (ЕС) 2024/1689 система, которая лишь проверяет текст и не принимает решений в отношении физических лиц, не входит в перечень систем высокого риска в правоохранительной сфере [17]; однако обработка ею персональных данных подозреваемых и несовершеннолетних требует мер защиты высокого уровня.

Главный риск внедрения – автоматизационная предвзятость: оператор склонен полагаться на систему и пропускать ошибки, о которых она не предупредила [21]; систематический обзор подтверждает, что этот эффект воспроизводится в разных сферах и снижается, когда пользователю понятны пределы системы и за ним сохраняется ответственность [22]. Применительно к нашей модели отсутствие предупреждения может восприниматься как подтверждение корректности сообщения, хотя по двум из тринадцати нарушений ассистент принципиально не способен их обнаружить. Поэтому интерфейс ассистента должен прямо указывать непроверяемые требования, а ответственное лицо – подтверждать их проверку самостоятельно. Исследователи полицейских алгоритмов также подчеркивают, что без независимой оценки и ясного распределения ответственности алгоритм воспроизводит ошибки исходных данных [10; 11]; для ассистента это означает обязательный журнал срабатываний и периодический анализ пропусков.

Второй риск – избыточная осторожность. Если ассистент будет только запрещать, пресс-служба получит формальный повод откладывать или сокращать сообщения. Правило полноты уравновешивает запреты требованием сообщить то, что раскрыть можно: факт события, принятые меры, квалификацию и процессуальный статус лица. Третий риск связан с генеративными функциями: если ассистент предлагает формулировки, должностное лицо обязано их редактировать и нести за них ответственность, а создание с помощью ИИ изображений или видеоматериалов к сообщениям о происшествиях недопустимо, поскольку синтетический контент подлежит обязательной маркировке [3] и подрывает доверие к официальному источнику.

С учетом изложенного предлагается трехуровневый порядок работы ассистента. «Красный» уровень: детерминированное срабатывание (имя или изображение несовершеннолетнего, оценочная формула о виновности конкретного лица, отсутствие источников помощи в сообщении о кризисной ситуации) блокирует направление текста на утверждение до исправления. «Желтый» уровень: вероятностное предупреждение (возможная косвенная идентификация, сведения о прошлом лица) требует письменного обоснования ответственного сотрудника. «Зеленый» уровень: срабатываний нет, текст направляется на утверждение с напоминанием о непроверяемых требованиях. Итоговый текст подписывается ЭЦП, журнал срабатываний хранится для анализа. После публикации ассистент отслеживает связанные события, прежде всего обнаружение разыскиваемого ребенка, и формирует задание на обновление ранее размещенного материала.

Заключение

Во-первых, законодательство Республики Казахстан, сформированное в 2025-2026 гг., допускает применение ИИ для предпубликационной проверки

официальных сообщений органов внутренних дел при условии сохранения решения за человеком, объяснимости срабатываний, функционирования в защищенном ведомственном контуре и защиты персональных данных.

Во-вторых, требования к официальным сообщениям поддаются формализации в виде десяти правил, охватывающих лексику презумпции невиновности, персональные данные, косвенную идентификацию несовершеннолетних, сведения о прошлом лица, сообщения о кризисных ситуациях, полноту сообщения, жизненный цикл публикации и опровержение слухов.

В-третьих, моделирование на материале пятнадцати эпизодов показало, что более половины выявленных нарушений обнаруживается детерминированными правилами, около трети – только в форме предупреждения для человека, а часть нарушений находится за пределами проверки текста. Наиболее тяжелые по последствиям ошибки автоматизируются хуже всего, что исключает полную замену профессиональной оценки.

В-четвертых, предложенный трехуровневый порядок работы ассистента с подписанием итогового текста ЭЦП может быть апробирован в пресс-службе МВД и одного территориального департамента полиции, а правила проверки – включены в программы подготовки сотрудников пресс-служб в Академии управления МВД Республики Казахстан. Перспективы исследования связаны с разработкой прототипа и его испытанием на расширенном корпусе сообщений с измерением доли пропусков и ложных срабатываний.

Список использованных источников

1 Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию»: от 8 сентября 2025 г. // https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-kazahstan-v-epohu-iskusstvennogo-intellekta-aktualnye-zadachi-i-ih-resheniya-cherez-cifrovuyu-transformaciyu-885145 (08.10.2026).

2 Указ Президента Республики Казахстан. Об объявлении Года цифровизации и искусственного интеллекта: от 6 января 2026 г., № 1151 // https://adilet.zan.kz/rus/docs/U2600001151 (08.10.2026).

3 Закон Республики Казахстан. Об искусственном интеллекте: от 17 ноября 2025 г., № 230-VIII // https://adilet.zan.kz/rus/docs/Z2500000230 (08.10.2026).

4 Кодекс Республики Казахстан. Цифровой кодекс Республики Казахстан: от 9 января 2026 г., № 255-VIII // https://adilet.zan.kz/rus/docs/K2600000255 (08.10.2026).

5 Закон Республики Казахстан. О кибербезопасности: от 24 ноября 2015 г., № 418-V // https://adilet.zan.kz/rus/docs/Z1500000418 (08.10.2026).

6 Сидорова Н.В., Серикбаев А.М. Цифровизация судебной и правоохранительной деятельности в Республике Казахстан // Вестник Карагандинского университета. Серия «Право». – 2023. – № 4(112). – С. 54-65.

7 Салимгерей А.А., Дуйсенов Э.Э., Байдаулетова А.И., Жумадилова Н.С. Закон Республики Казахстан «Об искусственном интеллекте»: проблемы реализации и образованности населения // Вестник КазНУ. Серия юридическая. – 2025. – Т. 115, № 3. – С. 43-52.

8 Саулен Н., Макарцев А.А., Тебаев Д.Б. Применение инструментов искусственного интеллекта в законодательном процессе и классическая парадигма законотворчества: проблемы интеграции // Вестник Института законодательства и правовой информации Республики Казахстан. – 2025. – Т. 80, № 2. – С. 235-244.

9 Талапина Э.В. Искусственный интеллект и правовые экспертизы в государственном управлении // Вестник Санкт-Петербургского университета. Право. – 2021. – Т. 12, вып. 4. – С. 865-881.

10 Babuta A., Oswald M. Data Analytics and Algorithmic Bias in Policing: Briefing Paper. – London: Royal United Services Institute, 2019.

11 Bennett Moses L., Chan J. Algorithmic prediction in policing: assumptions, evaluation, and accountability // Policing and Society. – 2018. – Vol. 28, No. 7. – P. 806-822.

12 INTERPOL, UNICRI. Toolkit for Responsible AI Innovation in Law Enforcement. Revised edition. – Lyon; Turin, 2024.

13 Закон Республики Казахстан. О персональных данных и их защите: от 21 мая 2013 г., № 94-V // https://adilet.zan.kz/rus/docs/Z1300000094 (08.10.2026).

14 Закон Республики Казахстан. О доступе к информации: от 16 ноября 2015 г., № 401-V // https://adilet.zan.kz/rus/docs/Z1500000401 (08.10.2026).

15 Кодекс Республики Казахстан. Уголовно-процессуальный кодекс Республики Казахстан: от 4 июля 2014 г., № 231-V // https://adilet.zan.kz/rus/docs/K1400000231 (08.10.2026).

16 Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment: CRC/C/GC/25, 2 March 2021.

17 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // https://eur-lex.europa.eu/eli/reg/2024/1689/oj (08.10.2026).

18 Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings // https://eur-lex.europa.eu/eli/dir/2016/343/oj (08.10.2026).

19 World Health Organization. Preventing suicide: a resource for media professionals, 2023 update. – Geneva: WHO, 2023.

20 European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. – Strasbourg: Council of Europe, 2018.

21 Parasuraman R., Manzey D.H. Complacency and Bias in Human Use of Automation: An Attentional Integration // Human Factors. – 2010. – Vol. 52, No. 3. – P. 381-410.

22 Goddard K., Roudsari A., Wyatt J.C. Automation bias: a systematic review of frequency, effect mediators, and mitigators // Journal of the American Medical Informatics Association. – 2012. – Vol. 19, No. 1. – P. 121-127.

ХАМЗЯЕВА ЮЛИЯ РАДИКОВНА
Начальник кафедры оперативно-розыскной деятельности
Казанского юридического института МВД России
кандидат юридических наук
подполковник полиции

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Использование искусственного интеллекта в деятельности правоохранительных органов – актуальная тема, продиктованная необходимостью поиска баланса между вызовами современности и назревшей потребностью повышения эффективности деятельности правоохранительных органов.

Преступность в современном мире все чаще характеризуется как «цифровая», что ставит перед правоохранительными органами принципиально новые задачи. Согласно статистическим данным МВД России, около 40 % преступлений в 2024 и 2025 года совершалось с использованием информационно-телекоммуникационных технологий [1] – кибератаки, мошенничество с криптовалютами, использование дипфейков и IoT-устройств. Традиционные методы раскрытия и расследования преступлений в подобных условиях являются малоэффетивными, что говорит о необходимости цифровизации всей правоохранительной деятельности, включая внедрение искусственного интеллекта [2, с. 18].

Внедрение искусственного интеллекта в правоохранительную деятельность может стать переходом на качественно новый уровень борьбы с преступностью. Генеральный прокурор РФ Игорь Краснов указывает, что искусственный интеллект «обладает существенным потенциалом для построения точных криминологических прогнозов», а его функционал позволяет «выявлять не всегда очевидные закономерности и риски роста противоправных угроз» [3]. Возможности искусственного интеллекта по обработке больших массивов данных, а также способность обнаруживать скрытые связи, имеют безусловный приоритет, когда традиционные методы выявления и расследования преступности всё чаще оказываются бессильными перед современной преступностью.

Одним из перспективных направлений внедрения искусственного интеллекта является оперативно-розыскная деятельность (далее ОРД). Но одновременно это направление является одним из наиболее проблемных. Оперативно-розыскная деятельность, в отличие от уголовно-процессуальной, обладает специфическими признаками: она носит разведывательно-поисковый характер, осуществляется преимущественно негласно и регламентируется ведомственными нормативными актами. Специфика оперативно-розыскной деятельности, с одной стороны позволяет более масштабно использовать искусственного интеллекта, с другой стороны, затрагивает правовую и этическую сторону данного направления.

Внедрение технологий искусственного интеллекта в оперативно-розыскную деятельность может позволить повысить ее эффективность по нескольким направлениям:

1. анализ большого объема данных и выявление скрытых связей и закономерностей. Сотрудникам оперативных подразделений при выполнении своих обязанностей, приходится работать с огромными массивами информации – данные систем связи, банковских транзакций, транспортных потоков, геолокационные метки, публикации в социальных сетях и мессенджерах. Как отмечает начальник Бюро специальных технических мероприятий МВД России генерал-лейтенант полиции А. Мошков, алгоритмы искусственного интеллекта позволяют выявлять закономерности в огромных массивах данных, что позволяет не только оперативно находить интересующую информацию, но и прогнозировать преступные намерения на ранних стадиях [4];
2. отождествление и идентификация. Системы биометрической идентификации на основе нейросетей могут более активно использоваться для распознавания лиц, голосов, почерка, автомобильных номеров и других уникальных признаков. Это позволит оперативно устанавливать личности фигурантов по фрагментарным данным, идентифицировать подозреваемых по записям камер видеонаблюдения и детально отслеживать перемещения интересующих лиц;
3. автоматизация мониторинга информационного пространства. ИИ-алгоритмы способны в круглосуточном режиме сканировать открытые источники, включая социальные сети, форумы и мессенджеры, выявляя признаки подготовки противоправных деяний, распространения запрещённой информации или вербовочной деятельности деструктивных групп и сообществ;
4. криминалистический анализ цифровых следов. Искусственный интеллект может помочь более эффективно обрабатывать изъятые цифровые носители, восстанавливать удалённую информацию, анализировать метаданные и выявлять аномалии в цифровых следах, что существенно повышает эффективность оперативно-технических мероприятий.

Несмотря на все положительные моменты, повсеместное внедрение технологий искусственного интеллекта в оперативно-розыскную деятельность сталкивается с определенными этическими и правовыми проблемами.

Основная проблема связана с правовой неопределенностью и отсутствием специального регулирования.

Что касается Российской Федерации, то Федеральный закон «Об оперативно-розыскной деятельности» № 144 от 12.08.1995 и ведомственные нормативные акты, принятые до повсеместного распространения технологий искусственного интеллекта, не предусматривают:

- понятийный аппарат и основные базовые дефиниции;
- порядок применения искусственного интеллекта в ходе оперативно-розыскных мероприятий и процедура пересмотра выводов, полученных с их помощью;
- требования к надёжности алгоритмов;

- ответственность за ошибки, которые привели к нарушению прав граждан.

Как справедливо отмечает А. Мошков, стремительное развитие научных технологий приводит к тому, что возникают новые средства, которые опережают законодательную базу, а в ряде случаев – нравственные устои общества [4].

Интересным представляется рассмотрение ситуации с нормативно-правовым регулированием использования технологий искусственного интеллекта в оперативно-розыскной деятельности в иных государствах. Учитывая общность границ, а также то, что «антикриминальное законодательство Казахстана и России, имея общие исторические корни, развивается в схожих направлениях и демонстрирует единство подходов в регламентации средств и методов борьбы с преступностью» [5, с. 196], рассмотрим опыт Республики Казахстан.

Регулирование использования технологий искусственного интеллекта в Республике Казахстан находится в стадии активного формирования. В январе 2026 года в стране вступил в силу Закон № 230-VIII ЗРК «Об искусственном интеллекте» от 17.11.2025, который заложил общие правовые рамки для всей рассматриваемой сферы. Он устанавливает правила пользования для любых систем искусственного интеллекта, включая используемые в правоохранительной деятельности.

Несмотря на наличие Закона, в общем регулирующего применение систем искусственного интеллекта, его прямое применение к ОРД связано с рядом проблем, на которые указывают как казахстанские [6], так и международные эксперты [7].

Одной из основных проблем является то, что Закон № 230-VIII ЗРК не учитывает специфику оперативно-розыскной деятельности, в частности, необходимость сохранения в тайне методов и источников информации. Требования к прозрачности алгоритмов искусственного интеллекта могут вступать в конфликт с принципом конспирации, лежащим в основе ОРД.

Очевидно, что назрела необходимость решения указанной проблемы в законах «Об оперативно-розыскной деятельности» союзных государств. В действующей редакции Закона Республики Казахстан № 154-XIII от 15.09.1994, принятого более 30 лет назад, отсутствует регулирование рассматриваемой деятельности. Однако проект нового закона «Об оперативно-розыскной деятельности» Казахстана выгодно отличается от своего предшественника.

Интересным и актуальным представляется выделение в Проекте закона «информационных» понятий и определений, таких как: цифровое пространство (среда), метаданные, мониторинг цифрового пространства (среды), анализ больших данных, блокчейн-анализ, цифровой трафик, цифровая активность, цифровая платформа, цифровой след. Также в проекте отдельно оговариваются особенности проведения оперативно-розыскных мероприятий в цифровом пространстве.

Рассмотрим некоторые из перечисленных определений.

Понятие «метаданные», по нашему мнению, является громоздким, содержащим большое количество родительных падежей: «характеристики, условия создания, способ передачи...». Определение описывает параметры, но не раскрывает саму суть метаданных. В данном случае допущена логическая ошибка «idem per idem», то есть «определение через определяемое»: метаданные – это

данные о данных, в Проекте закона дословно: «информация, описывающая... информацию».

Вероятно, более верным была бы следующая дефиниция: метаданные – сведения об электронных данных и коммуникациях (данные о данных), включающие структурированную информацию о времени, месте, отправителе, получателе, способе передачи и иных атрибутах. При этом содержание самой передаваемой информации не должно раскрываться.

В следующем рассматриваемом понятии «анализ больших данных (Big Data)», на наш взгляд, содержится грубая стилистико-логическая ошибка. Исходя из анализа слов «применение автоматизированных систем... для выявления», в дефиниции определяется метод, а не описывается процесс. Кроме того, здесь также допущена ошибка определения через определяемое: анализ – это применение систем для анализа.

Более корректным выглядит следующее определение: анализ больших данных (Big Data) – автоматизированный процесс обработки и сопоставления значительных массивов неструктурированной и структурированной информации, направленный на выявление скрытых закономерностей, прогнозирование тенденций и обнаружение факторов, представляющих оперативный интерес.

В понятии «блокчейн-анализ» допущена смысловая ошибка в виде подмены понятий. Исходя из сути определения, оно подходит к технологии «блокчейн», но не к анализу. По своей сути, блокчейн-анализ – это исследование цепочки транзакций, в том числе отслеживание движения криптовалют, анализ связей между адресами и т.д. А в определении, содержащимся в Проекте, описана архитектура распределенного реестра.

Если имеющееся в Проекте определение блокчейна дополнить определением анализа, то «блокчейн-анализ – совокупность методов и инструментов для исследования распределенных реестров (блокчейнов), позволяющих устанавливать связи между цифровыми адресами, отслеживать движение цифровых активов и идентифицировать участников транзакций в целях выявления противоправной деятельности».

Несмотря на все достоинства Проекта, законодательство Республики Казахстан, как и Российское законодательство, не содержит такие важные категории, как «разработчик», «дистрибьютор» или «интегратор» систем искусственного интеллекта [6]. В случае причинения ущерба в результате применения систем искусственного интеллекта, отсутствие в правовой доктрине указанных определений создает определенные сложности при разграничении ответственности между создателями систем и их пользователями в правоохранительных органах.

Наиболее корректным представляется внесение рассматриваемых понятий в Законы об оперативно-розыскной деятельности государств: России и Казахстана.

Одной из главных проблем при внедрении систем искусственного интеллекта в оперативно-розыскную деятельность, на наш взгляд, является соблюдение баланса между эффективностью использования систем и правами граждан. Как отмечают эксперты, основной задачей должно стать обеспечение равновесия между повышением эффективности правоохранительной деятельности за счет

использования искусственного интеллекта и защитой базовых прав граждан от дискриминации и непрозрачных решений [8].

Искусственные интеллект способен повысить скорость и качество сбора информации, но он не может заменить справедливость. Критерием оправданности использования систем искусственного интеллекта в оперативно-розыскной деятельности должна служить не только техническая точность полученных результатов, но и социальная направленность и безопасность.

Таким образом, необходима разработка специализированного правового регулирования, которое установит чёткие требования к системам искусственного интеллекта, внедряемым в ОРД, включая стандарты проверяемости алгоритмов, процедуры контроля и механизмы обжалования решений, принятых с использованием искусственного интеллекта. Также необходимо сформировать конкретные механизмы интеграции искусственного интеллекта в оперативно-розыскную деятельность, которые бы учитывали требования прозрачности и ответственности, но при этом не раскрывали оперативно значимую информацию.

Список литературы:

1. Сведения о состоянии преступности и результатах расследования преступлений: статистический сборник МВД России за 2024-2025 гг. URL: https://мвд.рф/reports/item/77848182/ (дата обращения: 26.08.2026).
2. Сардак Д.Б. Цифровая трансформация уголовно-процессуальной и экспертно-криминалистической деятельности // Российский следователь. 2026. № 6. С. 18-23.
3. Генпрокурор РФ Краснов указал на использование ИИ в борьбе с преступностью: выступление генерального прокурора РФ Игорь Краснов в ходе 7-й встречи руководителей прокурорских служб государств БРИКС. URL: https://amp.ren.tv/news/v-rossii/1367474-genprokuror-rf-krasnov-ukazal-na-ispolzovanie-ii-v-borbe-s-prestupnostiu (дата обращения: 26.08.2026).
4. Сотрудники БСТМ МВД России провели межрегиональный семинар-совещание об использовании искусственного интеллекта в правоохранительной деятельности: сообщение официального сайта МВД России. URL: https://мвд.рф/news/item/56938846/ (дата обращения: 26.08.2026).
5. Чечетин Е.А. Некоторые особенности законодательной регламентации оперативно-розыскных мероприятий в Республике Казахстан // Алтайский юридический вестник. 2025. № 3 (51). С. 195-201.
6. Хамидуллина Е., Грешников К. Актуальные вопросы регулирования искусственного интеллекта в Казахстане: обязанности, ответственность и практические рекомендации для бизнеса // ИС «Параграф». Статья от 23.06.2026. URL: https://prg.kz/document/?doc_id=35937018&pos=4;111 (дата обращения: 25.08.2026).
7. Kazakhstan’s New AI Regulatory Framework: краткий обзор законодательной базы Республики Казахстан по искусственному интеллекту // International Center for Not-for-Profit Law. 2025. URL: https:// https://www.icnl.org/post/news/kazakhstans-new-ai-regulatory-framework (дата обращения: 25.08.2026).
8. Адилов С.А. Цифровизация правоохранительной деятельности: реализация концепции продвижения идеологии закона и порядка // Вестник Волгоградской академии МВД России. 2025. № 4. С. 18-24.

ШАЛБАЕВ АЙДЫНГАЛИ ШАКРАТОВИЧ
Доцент кафедры специальной подготовки
Академии управления МВД Республики Казахстан
доктор философии (PhD)

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОГНОЗИРОВАНИЕ КАК ЭЛЕМЕНТ ТАКТИЧЕСКОГО МЫШЛЕНИЯ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Введение

Оперативно-розыскная деятельность по своему содержанию связана с необходимостью принятия решений в условиях неполноты информации, динамичности оперативной обстановки и вероятностного характера поведения лиц, представляющих оперативный интерес. В этих условиях особое значение приобретает способность оперативного сотрудника не только оценивать уже имеющиеся сведения, но и предвидеть возможное развитие событий. Предвидение выступает необходимым элементом аналитической работы, поскольку любое решение, в том числе тактическое, ориентировано на будущее и отвечает на вопрос о последующих действиях.

Одной из форм такого предвидения является оперативно-розыскное прогнозирование. Его содержание связано с использованием ранее собранной и систематизированной информации, знанием закономерностей развития преступного поведения, особенностей конкретных условий проведения оперативно-розыскных мероприятий, а также оценкой тактических возможностей оперативных сотрудников и иных участников оперативно-розыскной деятельности [1].

Актуальность рассмотрения оперативно-розыскного прогнозирования определяется тем, что качество прогностического вывода непосредственно влияет на содержание последующего тактического решения. В более широком криминологическом контексте прогнозирование связано с оценкой факторов риска и задачами предупреждения преступлений, что отражается в исследованиях зарубежного опыта криминологического обеспечения предупреждения преступлений и криминальной рискологии [2; 3]. Прогноз позволяет заранее учитывать возможное изменение оперативно-тактической ситуации, выбирать наиболее эффективные действия, определять необходимые средства и методы их реализации. В связи с этим прогнозирование следует рассматривать не как самостоятельный, изолированный элемент аналитической работы, а как составную часть тактического мышления оперативного сотрудника.

Целью настоящей статьи является рассмотрение сущности оперативно-розыскного прогнозирования, его информационно-логической основы и значения для формирования тактических решений в оперативно-розыскной деятельности.

1. Понятие и сущность оперативно-розыскного прогнозирования

Оперативно-розыскное прогнозирование относится к вероятностному виду предвидения. Его исходной основой выступают прошлый опыт и сведения о наличной ситуации, на базе которых формируются гипотезы о предстоящем

развитии событий. Каждой из таких гипотез может соответствовать определенная степень вероятности, а сам прогноз ориентирует субъекта оперативно-розыскной деятельности на подготовку к возможной ситуации [1].

Таким образом, прогнозирование не сводится к простому перечислению имеющихся фактов. При этом его информационная составляющая имеет значение и для оценки криминогенных факторов и рисков, рассматриваемых в современной криминологической литературе [3; 4]. Установленные сведения приобретают прогностическое значение только после их оценки и логического осмысления. Оперативный сотрудник устанавливает взаимосвязи между отдельными обстоятельствами, сопоставляет их с ранее известными закономерностями и на этой основе формирует представление о возможном развитии ситуации.

Существенным является и то обстоятельство, что оперативно-розыскное прогнозирование представляет собой результат мышления оперативного сотрудника. В процессе такого мышления решаются вопросы о том, каким образом может измениться оперативно-тактическая ситуация, какое поведение вероятно со стороны противоборствующей стороны и какие действия целесообразно предпринять в ожидаемой ситуации.

Результатом прогнозирования является прогнозный вывод, то есть достаточно четкая формулировка предполагаемого события или возможного направления развития ситуации. Прогнозный вывод стимулирует активность, способствует выбору эффективных и взаимосвязанных действий, позволяет учитывать необходимость отвлечения внимания и дезориентации противоборствующей стороны.

В связи с этим оперативно-розыскное прогнозирование целесообразно определить как информационно-логический процесс оценки имеющейся информации, выявления закономерностей и формирования вероятностного вывода о дальнейшем развитии оперативно-тактической ситуации и возможном поведении лиц, представляющих оперативный интерес, предшествующий принятию и влияющий на содержание тактического решения [1].

2. Оперативно-розыскное прогнозирование и тактическое мышление

Связь прогнозирования с тактическим мышлением проявляется прежде всего в последовательности интеллектуальных операций, которые осуществляет оперативный сотрудник. Сначала осуществляется получение и систематизация сведений, затем их оценка, выявление значимых связей и тенденций, после чего формируется прогнозный вывод. Полученный вывод, в свою очередь, служит основанием для выбора дальнейших действий.

Такое понимание позволяет рассматривать прогнозирование как промежуточное, но функционально значимое звено между информацией и тактическим решением. Любое тактическое решение обращено в будущее: оно должно учитывать не только существующее состояние объекта, но и вероятную реакцию лиц, изменение условий и последствия предпринимаемых действий. Поэтому прогнозирование обеспечивает предварительную оценку будущей ситуации.

Сложность прогнозирования может существенно различаться в зависимости от характера решаемой оперативной задачи. Оно может ограничиваться

элементарным предположением о вероятных действиях проверяемого или разрабатываемого лица на основе отдельного оперативного сообщения. Вместе с тем при сложной оперативной разработке требуется многовариантный расчет вероятных изменений оперативно-тактической ситуации. Тем самым уровни прогнозирования соответствуют уровням оперативно-розыскной тактики [1].

Особое значение прогноз приобретает в ситуациях, когда необходимо определить вероятное место, время или направление последующих действий. В подобных случаях совокупность сведений о ранее совершенных событиях, поведении конкретных лиц и условиях окружающей обстановки позволяет сформировать несколько возможных вариантов развития ситуации и определить наиболее вероятный из них.

Следовательно, тактическое мышление не может ограничиваться реакцией на уже произошедшие события. Его важной характеристикой является опережающий характер, предполагающий подготовку к возможным изменениям ситуации. Именно прогнозирование обеспечивает такую опережающую направленность оперативно-розыскной деятельности.

3. Информационная основа оперативно-розыскного прогнозирования

Качество прогноза непосредственно зависит от объема, достоверности, систематизированности и содержания исходной информации. В оперативно-розыскном прогнозировании может использоваться разнообразная информация, полученная от источников, в результате оперативно-розыскных мероприятий, следственных действий, из материалов дел оперативного учета, архивных материалов, а также из иных доступных источников [1].

Разнообразие решаемых задач обусловливает и разнообразие исходных сведений. Это могут быть данные о личности проверяемого или разрабатываемого лица, характеристиках оперативной обстановки, условиях функционирования конкретных объектов, особенностях территории, маршрутах передвижения, режиме работы объектов и другие сведения, способные повлиять на развитие прогнозируемой ситуации.

При этом отдельный факт сам по себе не всегда имеет достаточное прогностическое значение. Он приобретает такое значение в системе взаимосвязанных сведений. Чем полнее и точнее установлены связи между обстоятельствами, тем обоснованнее может быть прогнозный вывод. Следовательно, важнейшей задачей является не только получение информации, но и ее правильная оценка.

Информационная основа прогнозирования включает также знания о закономерностях преступного поведения. Для предвидения поведения конкретного лица может потребоваться учет его образа жизни, интересов, круга общения, преступного опыта, профессиональных навыков и психологических особенностей. При этом житейского опыта может быть достаточно для прогноза отдельных действий, однако для предвидения преступного поведения необходимы специальные знания о способах и механизмах совершения соответствующих преступлений [1].

Таким образом, прогнозирование предполагает соединение фактической информации со специальными знаниями. Такой подход согласуется с

необходимостью учитывать факторы риска и иные криминологически значимые обстоятельства при предупреждении преступлений [2; 3; 5]. В зависимости от конкретной ситуации могут иметь значение криминологические, психологические, медицинские, технические, экономические и иные знания. Их интеграция позволяет более полно учитывать факторы, способные повлиять на развитие событий.

4. Логические основы и методы прогнозирования

Логическая основа оперативно-розыскного прогнозирования включает несколько взаимодополняющих способов формирования прогностического вывода. К основным из них относятся экстраполяция, умозаключение по аналогии и моделирование [1]. Их применение определяется характером исходной информации и задачами, которые необходимо решить.

Экстраполяция представляет собой распространение установленных в прошлом тенденций на предстоящий период. Ее значение состоит в том, что повторяемость определенных связей и последовательностей позволяет предположить их возможное продолжение. В оперативно-розыскной деятельности такой подход может использоваться при анализе повторяющихся действий лиц, особенностей их поведения или условий, в которых происходили ранее установленные события.

Умозаключение по аналогии основано на перенесении знаний об изученных объектах и явлениях на новые объекты и явления, сходные с ними по существенным признакам. Применительно к ОРД аналогия позволяет использовать ранее накопленные знания о поведении преступников, способах реализации преступного замысла и характерных действиях после совершения определенных событий [1].

Моделирование предполагает исследование явлений и процессов посредством построения определенных моделей. В исходном материале в качестве таких моделей рассматриваются схемы межрегиональных связей, графическое отражение сроков и маршрутов, нанесение на карты местности и планы городов различных объектов, а также моделирование функций отдельных звеньев преступных групп. Значение моделирования заключается в возможности представить предполагаемое развитие ситуации в систематизированной форме и на этой основе получить прогностический вывод.

Указанные методы не являются взаимоисключающими. В сложных ситуациях они могут применяться одновременно. Экстраполяция позволяет установить тенденцию, аналогия – сопоставить ситуацию с ранее изученными случаями, а моделирование – представить возможные варианты развития событий. Их сочетание повышает обоснованность тактического предвидения.

5. Роль профессионального опыта и специальных знаний

Важной предпосылкой качества оперативно-розыскного прогнозирования является профессиональная подготовка и практический опыт оперативного сотрудника. В процессе профессиональной деятельности накапливаются знания о повторяющихся причинах и последствиях, типичных формах поведения, особенностях оперативной обстановки и тактических ситуаций. Поэтому с увеличением опыта расширяется возможность распознавания закономерностей, имеющих прогностическое значение [1].

Опыт, однако, не заменяет фактическую информацию. Его значение проявляется в способности правильно интерпретировать имеющиеся сведения и сопоставлять их с ранее известными ситуациями. Прогностический вывод становится более обоснованным тогда, когда конкретный факт получает объяснение в системе профессиональных знаний и подтверждается совокупностью взаимосвязанных обстоятельств.

Существенное значение имеет интеграция отраслевых знаний. Криминологическая и психологическая характеристика личности может позволить учитывать ее интересы, потребности и круг общения. В отдельных ситуациях могут иметь значение медицинские сведения, профессиональные навыки и иные обстоятельства, обусловливающие вероятное поведение лица. Использование таких знаний расширяет информационную основу прогнозирования и способствует более точному определению вероятного направления развития событий.

Профессиональный опыт особенно важен при формировании альтернативного прогноза. Если имеющаяся информация допускает несколько вариантов развития ситуации, оперативный сотрудник должен сопоставить их с известными закономерностями и определить наиболее вероятные варианты. Такой подход позволяет отказаться от однозначной оценки там, где фактическая обстановка объективно допускает различные сценарии.

6. Значение прогнозирования для принятия тактических решений

Практическое значение оперативно-розыскного прогнозирования наиболее полно проявляется на этапе принятия тактического решения. В этой связи результаты оценки криминальных рисков могут рассматриваться как один из информационных компонентов прогностической деятельности, в том числе применительно к вопросам ее правового обеспечения [5;6]. Прогнозный вывод задает направление последующих действий и влияет на выбор соответствующих средств и методов. Тем самым прогноз связывает аналитическую работу с практической реализацией поставленной оперативно-тактической задачи.

Важным результатом является повышение заблаговременности действий. Если оперативный сотрудник располагает обоснованным представлением о вероятном развитии ситуации, он получает возможность заранее подготовить соответствующие действия и учесть возможную реакцию противоборствующей стороны. Это позволяет сделать тактическое решение не только реактивным, но и опережающим.

Прогнозирование способствует также вариативности тактических решений. Поскольку оперативно-розыскная ситуация может развиваться по нескольким направлениям, целесообразно учитывать альтернативные варианты и заранее определять возможные действия применительно к каждому из них. Такой подход особенно значим при сложных оперативных ситуациях, в которых результат зависит от поведения нескольких взаимосвязанных лиц или изменения внешних условий.

При этом прогноз не должен рассматриваться как абсолютно достоверное описание будущего. Его вероятностный характер требует постоянного сопоставления прогностического вывода с вновь поступающей информацией.

Изменение исходных условий может потребовать корректировки первоначального прогноза и соответствующего изменения тактического решения.

Следовательно, эффективное оперативно-розыскное прогнозирование предполагает циклическую связь между информацией, прогнозом и решением: получение и систематизация сведений формируют прогноз, прогноз обусловливает тактическое решение, а результаты реализации решения и новые сведения становятся основанием для последующей оценки ситуации и уточнения прогностических выводов.

Заключение

Оперативно-розыскное прогнозирование представляет собой важнейший элемент тактического мышления в оперативно-розыскной деятельности. Его сущность заключается в информационно-логической обработке имеющихся сведений, использовании профессиональных знаний и опыта, выявлении закономерностей и формировании вероятностного вывода о дальнейшем развитии оперативно-тактической ситуации и поведении лиц, представляющих оперативный интерес.

Проведенный анализ позволяет выделить несколько взаимосвязанных характеристик прогнозирования. Во-первых, оно имеет вероятностный характер и поэтому предполагает оценку не только одного, но и нескольких возможных вариантов развития ситуации. Во-вторых, прогнозирование основывается на систематизированной информации и специальных знаниях. В-третьих, его логическую основу составляют экстраполяция, аналогия и моделирование. В-четвертых, качество прогноза во многом зависит от профессиональной подготовки и опыта оперативного сотрудника.

Особое значение имеет непосредственная связь прогнозирования с тактическим решением. В более широком контексте это соответствует подходу, при котором оценка криминальных рисков рассматривается как значимый элемент информационного обеспечения деятельности органов внутренних дел [5;6]. Прогнозный вывод позволяет заранее учитывать возможные изменения ситуации, выбирать наиболее эффективные направления действий и определять соответствующие средства и методы их реализации. Поэтому совершенствование способности к оперативно-розыскному прогнозированию является одним из условий повышения обоснованности и эффективности тактических решений.

В конечном счете оперативно-розыскное прогнозирование следует рассматривать как механизм перехода от анализа уже имеющейся информации к опережающему определению возможного развития событий. Его значение состоит не в безусловном предсказании будущего, а в формировании обоснованной вероятностной основы для подготовки и принятия тактических решений.

Список литературы:

1. Вероятностное прогнозирование деятельности человека. – М.: Наука, 1977. – С. 8.

2. Евсеев А.В. К вопросу о зарубежном опыте криминологического обеспечения предупреждения преступлений / А.В. Евсеев // Вестник ВИПК МВД России. – 2013. – № 3 (27). – С. 70–77.

3. Бабаев М.М., Пудовочкин Ю.Е. Феномен риска в контексте профилактической политики (криминальная рискология) // Вестник Санкт-Петербургского университета. – Серия «Право». – 2019. –

№ 1. – С. 136–148. – [Электронный ресурс]. – Режим доступа: https://doi.org/10.21638/spbu14.2019.110 (дата обращения 28.08.2026 г.).

4. Латентная преступность в Российской Федерации: 2001–2006: науч. издание / под ред. С.М. Иншакова. – М.: ЮНИТИ-ДАНА: Закон и право, 2007. – 351 с.

5. Латентная преступность как объект криминологического изучения. – [Электронный ресурс]. – Режим доступа: https://articlekz.com/article/20422 (дата обращения 28.08.2026 г.).

6. Шалбаев А.Ш. Правовое обеспечение оценки криминальных рисков в оперативно-розыскном законодательстве Республики Казахстан // Материалы дистанционной международной научно-практической конференции Карагандинской академии МВД РК им. Б. Бейсенова «Проблемы и перспективы совершенствования законодательства и правоприменительной практики органов внутренних дел».

ШАУДЫРОВ ТЕМИРБЕК САТЕМИРОВИЧ
докторант 2 курса Академии управления
МВД Республики Казахстан
магистр национальной безопасности и военного дела

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЦЕНТРОВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ: ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ УГОЛОВНОЙ ПРЕСТУПНОСТИ

Актуальность

Начну с того, что цифровая трансформация правоохранительной деятельности – это системный переход от бумажного и устного документооборота к единому цифровому контуру, в котором данные о происшествиях, обращениях граждан, видеонаблюдении и работе нарядов интегрированы между собой и доступны для аналитической обработки.

Применительно к Центру оперативного управления, или сокращенно ЦОУ, данный процесс приобретает особое значение, поскольку именно ЦОУ выступает узлом, через который проходит основной массив первичной оперативной информации органов внутренних дел.

Актуальность темы подтверждается принятием Закона Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года № 230-VIII ЗРК [1] и Концепции развития искусственного интеллекта Республики Казахстан на 2024-2029 годы, от 24 июля 2024 года № 592 [2], закрепляющих принципы ответственности, подконтрольности и объяснимости автоматизированных систем. Важно и то, что в Казахстане уже сформирована значительная цифровая инфраструктура – это система видеомониторинга «Сергек», охватывающая порядка 600 тысяч камер, и мобильное приложение «Police 102».

Вместе с тем хочу подчеркнуть ключевой тезис: накопление цифровых данных само по себе не равнозначно цифровой трансформации. Только последовательное внедрение технологий искусственного интеллекта способно превратить массив разрозненных сведений в реальный инструмент противодействия преступности.

Перейдем в содержательной части. Цифровую трансформацию ЦОУ, на наш взгляд, можно представить в виде трех последовательных этапов.

Первый этап – технологическое оснащение. На этом этапе отдельные процессы, такие как регистрация обращений, видеонаблюдение, навигация нарядов, переводятся в электронную форму, но не интегрируются между собой. Каждая система решает свою узкую задачу и не обеспечивает сквозного анализа происшествия.

Второй этап – интеграция цифровых контуров. Здесь электронная карточка происшествия, видеопоток, данные геолокации наряда и обращения через мобильное приложение объединяется в единой информационной среде ЦОУ. Оператор получает возможность видеть все сведения о событии одновременно.

Третий этап, и это ключевой момент доклада, – интеллектуализация. На этом этапе интегрированные данные подвергаются автоматизированной обработке

средствами искусственного интеллекта и машинного обучения с целью выявления закономерностей, формирования прогноза и поддержки принятия решения.

Хочу отметить, что третий этап определяет переход ЦОУ от цифровой, но все еще реактивной модели к модели интеллектуального ситуационного управления – модели, ориентированной уже не на фиксацию произошедшего, а на противодействие преступности. Казахстанская практика сегодня уверенно проходит переход от первого этапа ко второму, тогда как этап интеллектуализации требует отдельного целенаправленного развития.

Обратимся теперь к зарубежному опыту, который подтверждает, что цифровая трансформация оперативных центров полиции проходит аналогичные этапы.

Опыт Real-Time Crime Centers в Соединенных Штатах Америки показывает, что результативность подобных центров определяется способностью аналитического блока связывать разрозненные сигналы в единую картину развивающегося события, а не количеством установленных камер [5]. Британская система Gold-Silver-Bronze демонстрирует организационную модель, при которой данные распределяются по уровням управления – стратегическому, тактическому и оперативному – в зависимости от степени неопределенности ситуации [6]. Индийский опыт Integrated Command and Control Centres, реализуемый в рамках программы «100 умных городов», иллюстрирует еще более расширенную модель – объединение полиции, транспортной и коммунальной инфраструктуры на общей цифровой платформе [7].

Джерри Рэтклифф в своей концепции intelligence-led policing прямо указывает: цифровая трансформация полицейской деятельности измеряется способностью преобразовывать данные в приоритеты оперативного реагирования, а не их объемом [8]. При этом Питер Мэннинг предупреждает нас о риске того, что цифровизация способна порождать особую административную рациональность, при которой формальные показатели подменяют содержательную оценку ситуации [9]. Этот риск мы рассмотрим ниже.

Теперь перейдем к практическому вопросу – каким образом искусственный интеллект может применяться в деятельности ЦОУ Республики Казахстан. Мы выделяем три направления.

Первое направление – обработка обращений граждан: автоматическое распознавание речи, структурирование устных сообщений и предварительная классификация карточки происшествия по типу и степени срочности с использованием данных мобильного приложения «Police 102».

Второе направление – видеоаналитика на базе системы «Сергек»: автоматическое распознавание государственных регистрационных номерных знаков, выявление подозрительного поведения и скопления людей. Здесь важно подчеркнуть – плотность камер сама по себе не гарантирует снижение преступности без последующей аналитической обработки видеопотока [10]. Иными словами, от видеонаблюдения необходимо переходить именно к видеоаналитике.

Третье направление – пространственно-временной анализ криминогенной обстановки, основанный на накопленном массиве карточек происшествий и

позволяющий выявлять устойчивые «горячие точки», сезонные и суточные закономерности.

Криминологическое обоснование этих направлений мы находим в теории ситуационного предупреждения преступности Рональда Кларка [11] и в теории рационального выбора Дерека Корниша и Рональда Кларка [12]. Задача искусственного интеллекта здесь состоит не в замене человеческого решения, а в сокращении времени между появлением криминогенного сигнала и его профессиональной оценкой.

Полноценная цифровая трансформация ЦОУ невозможна без соответствующего организационно-правового обеспечения. Нормативную основу здесь составляют Закон Республики Казахстан «Об искусственном интеллекте» [1], Закон «О персональных данных и их защите» [3] и Закон «О кибербезопасности» [4].

В организационном плане необходимо, во-первых, привлечение в штат ЦОУ криминальных аналитиков и специалистов по обработке данных; во-вторых, разработка ведомственных стандартов подготовки операторов, работающих с системами поддержки принятия решений; в-третьих, установление многомерных показателей результативности ЦОУ – не только скорости реагирования, но и точности прогноза.

Перейдем к разделу, который считаю особенно важным для настоящей аудитории, – риски цифровой трансформации.

Первый риск – неравномерная достоверность данных: алгоритм обучается на основе уже накопленного массива сообщений, а неравномерная плотность наблюдения способна воспроизводить и усиливать уже существующее неравенство наблюдаемости отдельных территорий.

Второй риск – алгоритмическая ошибка: автоматически сформированная рекомендация может основываться на неполных данных, а сотрудник, формально сохраняя право ее скорректировать, фактически способен испытывать эффект предустановленного выбора.

Третий риск – избыточная обработка персональных данных, возрастающая по мере интеграции цифровых контуров ЦОУ.

И четвертый риск, о котором упоминалось – снижение профессионального суждения сотрудника, когда формальный показатель начинает подменять содержательную оценку ситуации. Поэтому мы настаиваем: при проектировании цифровых решений для ЦОУ необходимо сохранять объяснимость алгоритмических рекомендаций и персональную ответственность должностного лица за итоговое решение.

Заключение

Цифровая трансформация ЦОУ – это последовательный процесс перехода от точечного технологического оснащения через интеграцию цифровых контуров к интеллектуализации деятельности на основе искусственного интеллекта. И только последний этап обеспечивает переход от фиксации происшествий к реальному противодействию преступности.

В связи с чем предлагается первое – завершить интеграцию цифровых контуров ЦОУ в единую информационную среду; второе – поэтапно внедрять

видеоаналитику и пространственно-временной анализ на базе уже существующей инфраструктуры «Сергек»; третье – ввести в штат ЦОУ должности криминальных аналитиков и специалистов по обработке данных; четвертое – закрепить ведомственными актами МВД требования объяснимости и подконтрольности алгоритмических рекомендаций; пятое – провести пилотные проекты цифровой трансформации на ограниченной территории с последующей научной оценкой их результативности перед тиражированием на республиканском уровне.

Список литературы:

1. Об искусственном интеллекте : Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК // Информационно-правовая система «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 24.08.2026).
2. Об утверждении Концепции развития искусственного интеллекта на 2024-2029 годы : постановление Правительства Республики Казахстан от 24 июля 2024 года № 592 // Информационно-правовая система «Әділет». – URL: https://adilet.zan.kz/rus/docs/P2400000592 (дата обращения: 24.08.2026).
3. О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 года № 94-V // Информационно-правовая система «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 24.08.2026).
4. О кибербезопасности : Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК // Информационно-правовая система «Әділет». – URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 24.08.2026).
5. Real-Time Crime Centers : Integrating Technology to Enhance Public Safety. – Washington, DC : National Institute of Justice, April 2025. – NCJ 310472.
6. Pearce T., Fortune J. Command and control in policing : a systems assessment of the gold, silver and bronze structure // Journal of Contingencies and Crisis Management. – 1995. – Vol. 3. – No. 3. – P. 181-187.
7. Praharaj S. Command and control governance in the 100 smart cities mission in India : Urban innovation or utopias? // Applied Geography. – 2025. – Vol. 184. – Article 103766.
8. Ratcliffe J.H. Intelligence-Led Policing. – 2nd ed. – London ; New York : Routledge, 2016.
9. Manning P.K. The Technology of Policing : Crime Mapping, Information Technology, and the Rationality of Crime Control. – New York : New York University Press, 2008.
10. Эффективность камер «Сергек» обсудили в МВД // Polisia.kz : ведомственный информационный портал Министерства внутренних дел Республики Казахстан. – 1 июля 2022 года. – URL: https://polisia.kz/ru/effektivnost-kamer-sergek-obsudili-v-mvd/ (дата обращения: 24.08.2026).
11. Clarke R.V. Situational Crime Prevention : Successful Case Studies. – 2nd ed. – Albany: Harrow and Heston, 1997.
12. Cornish D.B., Clarke R.V. The Reasoning Criminal : Rational Choice Perspectives on Offending. – New York : Springer-Verlag, 1986.

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясының қорытындысы бойынша ҰСЫНЫМДАР

Конференция материалдарында баяндалған ғылыми тұжырымдар мен практикалық ұсыныстарды қорыту негізінде қылмыстылыққа қарсы іс-қимыл саласында жасанды интеллект технологияларын заңды, қауіпсіз және тиімді қолдануды дамыту мақсатында мынадай ұсынымдар қалыптастырылды:

1. **Ішкі істер органдарының қызметінде, жедел-іздестіру қызметінде және сотқа дейінгі тергеп-тексеруде жасанды интеллектіні қолданудың ведомстволық нормативтік және әдістемелік негіздерін жетілдіру**, онда жасанды интеллект жүйелерін қолданудың рұқсат етілген бағыттарын, олардың нәтижелерінің құқықтық мәртебесін, алгоритмдік өңдеу нәтижелерін тіркеу, құжаттау, тексеру және бағалау тәртібін, сондай-ақ әзірлеушілердің, жүйе иеленушілерінің, әкімшілер мен пайдаланушылардың жауапкершілік шектерін айқындау.
2. **Адамның міндетті бақылауы қағидатын сақтау**, оған сәйкес жасанды интеллект нәтижелері ақпараттық-талдамалық және көмекші құрал ретінде пайдаланылуға тиіс, ал адамның құқықтары мен бостандықтарына әсер ететін заңдық маңызы бар шешімдер тек уәкілетті лауазымды тұлғамен қабылданып, оның заңдылығы мен негізділігі үшін дербес жауапкершілік сақталуы қажет. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации
3. **Құқық қорғау органдарында қолданылатын жасанды интеллект жүйелерін бақылау және аудиттеу тетігін қалыптастыру**, алгоритмдердің жұмысын міндетті хаттамалауды, олардың дәлдігін, түсіндірмелілігін, ықтимал кемсітушілік ауытқуларын, ақпараттық қауіпсіздігін және дербес деректерді қорғау талаптарына сәйкестігін мерзімді тексеруді көздеу. Жоғары тәуекелді жүйелер үшін тәуелсіз немесе ведомствоаралық сараптамалық бағалау мүмкіндігін қарастыру. Сборник МНПК_для рекомендации
4. **Цифрлық дәлелдемелермен және жасанды интеллектіні пайдалану арқылы алынған криминалистикалық нәтижелермен жұмыс істеудің бірыңғай әдістемелік тәсілдерін қалыптастыру**, цифрлық объектінің бастапқы көзін, метадеректерін, тұтастығын, сақтау және беру тізбегін, жүргізілген операцияларды және зерттеу нәтижелерінің қайта тексерілуі мен қайталанғыштығын қамтамасыз ету. Цифрлық криминалистика бойынша ведомствоаралық әдістемелік базаны дамыту. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации
5. **Жасанды интеллект арқылы жасалған немесе өзгертілген фото-, бейне- және аудиоматериалдарды, оның ішінде deepfake және spoofing технологияларын анықтау әдістемелерін дамыту**, автоматтандырылған талдау нәтижелерін міндетті сараптамалық тексерумен ұштастыру және мұндай нәтижелерді дәлелдемелік мақсатта пайдалану кезінде олардың сенімділігі мен тексерілуін қамтамасыз ету. Сборник МНПК_для рекомендации

6. **OSINT құралдарын жедел-іздестіру қызметінде қолданудың құқықтық және әдістемелік негіздерін нақтылау**, ашық дереккөздерден ақпарат жинау мен талдаудың құқыққа сай шектерін, жалпыға қолжетімді ақпарат пен қолжетімділігі шектеулі мәліметтердің ара-жігін, дереккөзді, метадеректерді және цифрлық объектінің тұтастығын тіркеу, алынған мәліметтерді верификациялау және құжаттау талаптарын белгілеу. Сборник МНПК_для рекомендации

7. **Әлеуметтік желілерде, мессенджерлерде және өзге де цифрлық платформаларда есірткіге байланысты заңға қайшы контентті, жасырын жарнаманы және есірткі бизнесіне тарту белгілерін анықтау үшін жасанды интеллект негізіндегі автоматтандырылған мониторинг пен парсинг құралдарын дамыту**, сондай-ақ цифрлық платформалар әкімшіліктерімен мұндай контентті жедел анықтау, сақтау, бұғаттау және жою жөніндегі өзара іс-қимылды жетілдіру. Сборник МНПК_для рекомендации

8. **Киберқылмыстылыққа қарсы халықаралық ынтымақтастықтың жедел тетіктерін нығайту**: тәулік бойы жұмыс істейтін байланыс арналары мен байланыс пункттерін дамыту, электрондық ақпаратты жедел сақтау және алмасу рәсімдерін жетілдіру, трансұлттық киберқылмыстар бойынша бірлескен талдамалық және тергеу топтарын құру, сондай-ақ электрондық дәлелдемелер мен цифрлық криминалистика саласындағы тәсілдерді үйлестіру. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации

9. **Құқық қорғау органдарының қаржы ұйымдарымен, байланыс операторларымен, цифрлық платформалармен, технологиялық компаниялармен және киберқауіпсіздік саласындағы ұйымдармен тұрақты өзара іс-қимылын кеңейту**, киберқауіптер, күмәнді операциялар, аккаунттар, цифрлық инфрақұрылым және жаңа қылмыстық схемалар туралы ақпарат алмасу мен жедел ден қою тетіктерін дамыту. Сборник МНПК_для рекомендации

10. **Интернет-алаяқтық пен дропперліктің ерте профилактикасы үшін жасанды интеллект пен предиктивтік талдау мүмкіндіктерін дамыту**, оның ішінде күмәнді қаржылық операцияларды, цифрлық коммуникацияларды, қайталанатын мінез-құлық үлгілерін және кәмелетке толмағандарды «жеңіл табыс» түріндегі ұсыныстар арқылы тарту белгілерін анықтау. Алгоритмдік тәуекел индикаторлары профилактикалық тексеруге негіз болуға тиіс, бірақ адамның кінәлілігінің дәлелі ретінде қарастырылмауы қажет. Сборник МНПК_для рекомендации

11. **Ішкі істер органдарының ақпараттық жүйелері мен жедел басқару орталықтарының деректерін қауіпсіз бірыңғай талдамалық ортада кезең-кезеңімен ықпалдастыру**, заңда белгіленген қолжетімділік режимдерін сақтай отырып, оқиғалар, азаматтардың өтініштері, бейнебақылау, жедел және өзге де ақпаратты интеллектуалдық талдау, объектілер арасындағы жасырын байланыстарды анықтау және байланыстар графтарын құру мүмкіндігін дамыту. Бұл ретте деректердің сапасы, өзектілігі, ақпараттық жүйелердің үйлесімділігі және ақпараттық қауіпсіздік қамтамасыз етілуі тиіс. Сборник МНПК_для рекомендации

12. **Криминологиялық және жедел-талдамалық болжау құралдарын шешім қабылдауды қолдау құралы ретінде дамыту**, оларды қылмыстық тәуекелдерді, кеңістіктік-уақыттық заңдылықтарды, байланыстарды және

профилактикалық жұмыстың басым бағыттарын айқындау үшін пайдалану. Ықтималдық сипатындағы алгоритмдік болжам адамның құқықтарын шектеудің немесе кінәлілігі туралы қорытындының дербес негізіне айналмауға тиіс. Сборник МНПК_для рекомендации

13. **Критикалық ақпараттық инфрақұрылымның киберорнықтылығын күшейту**, тұрақты мониторингті, желілерді сегменттеуді, қолжетімділікті бақылауды, деректердің резервтік көшірмесін жасауды, бағдарламалық қамтамасыз етуді уақтылы жаңартуды, кибершабуыл сценарийлері бойынша жүйелі стресс-тестілеуді, инциденттерге ден қою және қалпына келтіру рәсімдерін, сондай-ақ мемлекеттік органдар мен инфрақұрылым операторлары арасындағы киберқауіптер туралы ақпарат алмасуды дамыту. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации

14. **Қазақстан Республикасы ІІМ Басқару академиясының ғылыми-білім беру әлеуетін пайдалана отырып, құқық қорғау қызметіне арналған жасанды интеллект саласындағы қолданбалы зерттеулер мен пилоттық жобаларды жүйелі дамыту**, отандық технологиялық шешімдерді әзірлеу және сынау үшін Академияның, практикалық бөлімшелердің, киберполицияның, ғылыми ұйымдар мен IT-компаниялардың ынтымақтастығын кеңейту. Әрбір пилоттық жоба үшін күтілетін нәтиже, тиімділік пен қауіпсіздікті бағалау өлшемшарттары алдын ала белгіленуге тиіс. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации

15. **Құқық қорғау органдары қызметкерлерін даярлау және қайта даярлау жүйесін жаңғырту**, білім беру бағдарламаларына жасанды интеллектіні құқықтық және этикалық тұрғыдан қолдану, цифрлық криминалистика, деректерді талдау, киберқауіпсіздік, OSINT, фактчекинг, дербес деректерді қорғау және алгоритм нәтижелерін тексеру бойынша оқу модульдерін енгізу; киберполигондарды, практикалық кейстерді және модельденген цифрлық инциденттерді кеңінен пайдалану. Сборник МНПК_для рекомендации Сборник МНПК_для рекомендации

16. **Жасанды интеллектіні жауапты және қауіпсіз қолданудың бірыңғай этикалық-ұйымдастырушылық стандарттарын қалыптастыру**, оларда заңдылық, әділдік, кемсітушілікке жол бермеу, деректерді барынша аз пайдалану, құпиялылық, түсіндірмелілік, ақпараттық қауіпсіздік, адамның бақылауы және кәсіби жауапкершілік қағидаттарын бекіту. Тиісті құқықтық негізсіз дербес деректерді, қызметтік және қолжетімділігі шектеулі ақпаратты жалпыға қолжетімді жасанды интеллект сервистеріне беруге жол бермеу және ведомстволық білім беру мен қызметтік ортада ИИ пайдалану қағидаларын әзірлеу.

17. **Жедел-іздестіру психологиясын ішкі істер органдарының жедел бөлімшелері қызметкерлерін кәсіби даярлаудың және қолданбалы ғылыми зерттеулердің дербес бағыты ретінде жүйелі түрде дамыту.** Ведомстволық білім беру бағдарламаларына **«Жедел-іздестіру психологиясы»** арнайы курсын енгізу, онда адамдармен кәсіби қарым-қатынас жасау, құпия ынтымақтастықты ұйымдастырудың психологиялық аспектілері, әлеуметтік инженерия әдістерін тану және оларға қарсы іс-қимыл, сондай-ақ жедел бөлімшелердегі қолайлы кәсіби-психологиялық ахуалды қалыптастыру мәселелерін қамту ұсынылады. Дәстүрлі

психологиялық әдістерді жасанды интеллект, OSINT және үлкен деректерді талдау мүмкіндіктерімен ұштастыра отырып, жедел қызметкерлердің адамдармен жұмыс істеу, мінез-құлық ерекшеліктерін бағалау және заманауи ұйымдасқан әрі технологиялық қылмыстылыққа қарсы іс-қимыл жасау құзыреттерін жетілдіру қажет.

18. **Жедел-іздестіру қызметі теориясын заманауи қылмыстылыққа қарсы іс-қимылдың ғылыми негізі ретінде дамыту және ведомстволық ғылымның практикалық бөлімшелермен байланысын күшейту.** Жедел-іздестіру қызметіне ақпараттық және цифрлық технологияларды енгізудің стратегиялық бағыттарын айқындау, киберкеңістіктегі құқыққа қайшы мінез-құлықты, жасанды интеллект мүмкіндіктерін және өзге де жаңа технологиялық факторларды жедел-іздестіру ғылымының зерттеу пәніне жүйелі түрде енгізу ұсынылады. Практикалық бөлімшелердің нақты сұраныстары негізінде ғылыми негізделген ұсынымдар, алгоритмдер мен қолданбалы шешімдер әзірлеуді жолға қою, озық жедел тәжірибені жинақтау және барлық жедел-іздестіру субъектілері ғалымдарының күш-жігерін Қазақстандағы бірыңғай жедел-іздестіру теориясын дамытуға шоғырландыру қажет.

РЕКОМЕНДАЦИИ
по итогам международной научно-практической конференции «Искусственный интеллект в противодействии преступности»

По результатам обобщения научных выводов и практических предложений, изложенных в материалах конференции, в целях развития законного, безопасного и эффективного применения технологий искусственного интеллекта в сфере противодействия преступности сформулированы следующие рекомендации:

1. **Совершенствовать ведомственную нормативную и методическую основу применения искусственного интеллекта в деятельности органов внутренних дел, оперативно-розыскной деятельности и досудебном расследовании**, определив допустимые направления использования систем ИИ, правовой статус получаемых результатов, порядок фиксации, документирования, проверки и оценки результатов алгоритмической обработки, а также пределы ответственности разработчиков, владельцев систем, администраторов и пользователей.
2. **Обеспечить обязательный человеческий контроль**, при котором результаты работы искусственного интеллекта используются в качестве информационно-аналитического и вспомогательного инструмента, а юридически значимые решения, способные затрагивать права и свободы человека, принимаются исключительно уполномоченным должностным лицом с сохранением его персональной ответственности за законность и обоснованность решения.
3. **Сформировать механизм контроля и аудита систем искусственного интеллекта, применяемых правоохранительными органами**, предусматривающий обязательное протоколирование работы алгоритмов, периодическую проверку их точности, объяснимости, возможной алгоритмической предвзятости, информационной безопасности и соответствия требованиям защиты персональных данных. Для систем высокого риска предусмотреть возможность независимой либо межведомственной экспертной оценки.
4. **Сформировать единые методические подходы к работе с цифровыми доказательствами и криминалистическими результатами, полученными с использованием искусственного интеллекта**, обеспечив фиксацию исходного источника цифрового объекта, сохранение метаданных, целостности и цепочки хранения и передачи, документирование выполненных операций, а также проверяемость и воспроизводимость результатов исследования. Развивать межведомственную методическую базу цифровой криминалистики.
5. **Развивать методики выявления фото-, видео- и аудиоматериалов, созданных либо модифицированных с использованием искусственного интеллекта, включая технологии deepfake и spoofing**, сочетая автоматизированную детекцию с обязательной экспертной проверкой и обеспечивая надежность и проверяемость таких результатов при их использовании в доказывании.
6. **Уточнить правовые и методические основы применения OSINT в оперативно-розыскной деятельности**, определив правомерные пределы сбора и анализа информации из открытых источников, разграничение общедоступной

информации и сведений ограниченного доступа, а также требования к фиксации источника, метаданных и целостности цифрового объекта, верификации и документированию полученной информации.

7. **Развивать автоматизированные средства мониторинга и парсинга на основе искусственного интеллекта для выявления противоправного контента, связанного с наркотиками, скрытой наркорекламы и признаков вовлечения в наркобизнес в социальных сетях, мессенджерах и иных цифровых платформах**, одновременно совершенствуя взаимодействие с администрациями цифровых платформ по оперативному выявлению, сохранению, блокированию и удалению такого контента.

8. **Укреплять оперативные механизмы международного сотрудничества в противодействии киберпреступности**: развивать круглосуточные каналы и контактные пункты, совершенствовать процедуры оперативного сохранения и обмена электронной информацией, создавать совместные аналитические и следственные группы по транснациональным киберпреступлениям, гармонизировать подходы к электронным доказательствам и цифровой криминалистике.

9. **Расширять постоянное взаимодействие правоохранительных органов с финансовыми организациями, операторами связи, цифровыми платформами, технологическими компаниями и организациями в сфере кибербезопасности**, развивая обмен информацией о киберугрозах, подозрительных операциях, аккаунтах, цифровой инфраструктуре и новых преступных схемах, а также механизмы оперативного реагирования.

10. **Развивать возможности искусственного интеллекта и предиктивной аналитики для ранней профилактики интернет-мошенничества и дропперства**, в том числе среди несовершеннолетних, путем выявления подозрительных финансовых операций, цифровых коммуникаций, повторяющихся моделей поведения и признаков вовлечения в противоправные схемы под видом «легкого заработка». Алгоритмические индикаторы риска должны использоваться для профилактической проверки, но не рассматриваться как доказательство виновности лица.

11. **Поэтапно интегрировать данные информационных систем органов внутренних дел и центров оперативного управления в защищенную единую аналитическую среду**, обеспечивая в пределах установленных законом режимов доступа интеллектуальный анализ сведений о происшествиях, обращениях граждан, видеонаблюдении, оперативной и иной информации, выявление скрытых взаимосвязей и построение графов связей. Одновременно необходимо обеспечивать качество и актуальность данных, совместимость информационных систем и информационную безопасность.

12. **Развивать криминологическое и оперативно-аналитическое прогнозирование как инструмент поддержки принятия решений**, используя его для выявления криминальных рисков, пространственно-временных закономерностей, взаимосвязей и определения приоритетных направлений профилактической работы. Вероятностный алгоритмический прогноз не должен

становиться самостоятельным основанием для ограничения прав человека либо вывода о его виновности.

13. **Укреплять киберустойчивость критической информационной инфраструктуры**, развивая постоянный мониторинг, сегментацию сетей, контроль доступа, резервное копирование данных, своевременное обновление программного обеспечения, регулярное стресс-тестирование по сценариям кибератак, процедуры реагирования на инциденты и восстановления, а также обмен информацией о киберугрозах между государственными органами и операторами инфраструктуры.

14. **Системно развивать прикладные исследования и пилотные проекты в области искусственного интеллекта для правоохранительной деятельности с использованием научно-образовательного потенциала Академии управления МВД Республики Казахстан**, расширяя сотрудничество Академии, практических подразделений, киберполиции, научных организаций и IT-компаний в разработке и испытании отечественных технологических решений. Для каждого пилотного проекта целесообразно заранее определять ожидаемый результат и критерии оценки эффективности и безопасности.

15. **Модернизировать систему подготовки и переподготовки сотрудников правоохранительных органов**, включая в образовательные программы модули по правовым и этическим основам применения искусственного интеллекта, цифровой криминалистике, анализу данных, кибербезопасности, OSINT, фактчекингу, защите персональных данных и проверке алгоритмических результатов; шире использовать киберполигоны, практические кейсы и моделирование цифровых инцидентов.

16. **Сформировать единые этические и организационные стандарты ответственного и безопасного использования искусственного интеллекта**, закрепив принципы законности, справедливости, недопущения дискриминации, минимизации данных, конфиденциальности, объяснимости, информационной безопасности, человеческого контроля и профессиональной ответственности. Не допускать передачи персональных данных, служебной и иной информации ограниченного доступа в общедоступные сервисы ИИ без соответствующего правового основания и разработать внутренние правила использования ИИ в образовательной и служебной деятельности.

17. **Системно развивать оперативно-розыскную психологию как самостоятельное направление профессиональной подготовки сотрудников оперативных подразделений органов внутренних дел и прикладных научных исследований.** Предусмотреть в программах ведомственного образования специальный курс **«Оперативно-розыскная психология»**, охватывающий профессиональное взаимодействие с людьми, психологические аспекты организации конфиденциального сотрудничества, распознавание и противодействие методам социальной инженерии, а также формирование благоприятного профессионально-психологического климата в оперативных подразделениях. Совершенствовать компетенции оперативных сотрудников по работе с людьми, оценке особенностей поведения и противодействию современным организованным и технологичным формам преступности путем сочетания

традиционных психологических методик с возможностями искусственного интеллекта, OSINT и анализа больших данных.

18. **Развивать теорию оперативно-розыскной деятельности как научную основу современного противодействия преступности и укреплять связь ведомственной науки с практическими подразделениями.** Определить стратегические направления внедрения информационных и цифровых технологий в оперативно-розыскную деятельность, системно включать в предмет исследований оперативно-розыскной науки вопросы противоправного поведения в киберпространстве, возможностей искусственного интеллекта и иных новых технологических факторов. Организовать разработку по конкретным запросам практических подразделений научно обоснованных рекомендаций, алгоритмов и прикладных решений, обобщение передового опыта оперативной практики, а также консолидацию научного потенциала субъектов ОРД для дальнейшего развития единой оперативно-розыскной теории в Казахстане.

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясынан естелік фотолар





МАЗМҰНЫ
СОДЕРЖАНИЕ

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясы бағдарламасы 4-6
Программа международной научно-практической конференции «Искусственный интеллект в противодействии преступности» 7-9

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясына қатысушылар тізімі 10-12

Список участников международной научно-практической конференции «Искусственный интеллект в противодействии преступности» 12-14

КІРІСПЕ СӨЗ / ПРИВЕТСТВЕННОЕ СЛОВО
Дильбарханова Ж.Р. 15-16
Алимова Э.А. 17-18
Гриценко В.В. 19-20
Биржанов Б.К. 21-25
Тургульдинов Р.А. 26-29
Рапишев Д.А. 30-35

БАЯНДАМАЛАР
ДОКЛАДЫ

АБДУЛЛОЗОДА Н.Р.
Трансформация оперативно-розыскного противодействия молодежному экстремизму в условиях цифровизации и внедрения систем искусственного интеллекта (на примере Республики Таджикистан) — 36–41

АБЕНОВ А.А.
Цифровая криминалистика и интеллектуальная обработка данных в экспертно-криминалистическом обеспечении противодействия уголовной преступности в Республике Казахстан — 42–46

АБЕНОВ Р.Т.
Искусственный интеллект в оперативно-розыскной деятельности и досудебном расследовании — 47–52

АЙДАРОВА А.А.
Искусственный интеллект в противодействии уголовной преступности: опыт и перспективы применения в оперативно-розыскной деятельности и досудебном расследовании Республики Казахстан — 53–59

АХМЕТОВ К.Р.
Искусственный интеллект как инструмент анализа цифровых следов при расследовании киберпреступлений в Казахстане — 60–66

БАЗАРБАЕВА А.Б.
Возможности искусственного интеллекта в профилактике правонарушений и совершенствовании профессиональной подготовки сотрудников органов внутренних дел — 67–70

БУЗАКАНОВА А.Б.
Формирование культуры ответственного использования искусственного интеллекта обучающимися: правовые и этические аспекты — 71–77

ГАЛИЕВ С.Ж.
Противодействие преступности в современный период: роль теории ОРД — 78–84

ГЛУБОКОВСКИХ Р.В.
Искусственный интеллект в оперативно-розыскном прогнозировании: правовые, организационные и этические аспекты внедрения — 85–91

ГРИНЕВА Д.А.
Система учетов органов внутренних дел: проблемы и пути совершенствования — 92–96

ДЖИГИТОВА Р.Н.
Қылмыстық құқық бұзушылықтарға қарсы іс-қимылдағы жасанды интеллект: тарихи дамуы және Қазақстан тәжірибесі — 97–102

ДЮСЕБЕКОВА С.Б.
Цифровое поведение сотрудника полиции как фактор профессиональной безопасности при использовании искусственного интеллекта — 103–107

ЕСЕНБАЕВА А.Л.
Кибербезопасность критической инфраструктуры Республики Казахстан: современные угрозы и механизмы защиты — 108–114

ЖАНХАН Н.Ж.
Жедел-іздестіру қызметін ақпараттық-талдамалық қамтамасыз етуде жасанды интеллектіні қолданудың құқықтық және ұйымдастырушылық негіздері — 115–121

ЖАРЫЛКАСЫНОВ К.Ә.
Искусственный интеллект в правоохранительной системе Казахстана: модели, направления применения — 122–126

ЖОЛШЫБАЙ Ә.Қ.
Искусственный интеллект в исследовании фото- и видеоматериалов: современные возможности и криминалистические задачи — 127–130

ЖУМАБАЕВ М.А.
Актуальные проблемы оперативно-розыскной деятельности: теория, законодательство и правоприменительная практика в условиях цифровизации — 131–136

ЖУНИСБЕКОВ Н.Н.
Правовые и процессуальные аспекты применения OSINT в оперативно-розыскной деятельности — 137–143

ИСКАКОВ А.К.
К вопросу о становлении оперативно-розыскного права как самостоятельной юридической науки — 144–148

КАНАШЕВ А.М.
Электронные доказательства в расследовании киберпреступлений в Республике Казахстан: проблемы собирания, проверки и использования — 149–154

КАРЛ А.М., ШАХМАТОВ А.В.
Оперативно-розыскная деятельность в условиях цифровизации: роль и место кибербезопасности — 155–158

КАУАЗОВ С.К.
Реконструкция событий по цифровым следам в современной криминалистике: возможности и проблемы применения в Республике Казахстан — 159–165

КАУНОВ А.В.
Использование современных технических возможностей в противодействии организованной преступности на территории Российской Федерации — 166–169

КЕНЖЕЕВ С.С.
Искусственный интеллект и интеллектуальный анализ данных как инструменты совершенствования исследования вещественных доказательств в цифровой криминалистике — 170–175

КОНВИСАРЬ А.А.
Этико-организационные риски внедрения искусственного интеллекта в правоохранительную деятельность: баланс между эффективностью и защитой прав человека — 176–182

КРАВЦОВА Ю.А.
Этика использования искусственного интеллекта в правоохранительной деятельности — 183–188

КУСАИНОВА А.М.
Искусственный интеллект в исследовании и цифровой реконструкции следов создания помех управлению воздушным судном — 189–192

КУШЕНОВ А.М.
Предиктивные технологии искусственного интеллекта в профилактике интернет-мошенничества и дропперства среди несовершеннолетних в Республике Казахстан — 193–198

ҚУАНЫШБЕККЫЗЫ Г.
Цифрлық дәлелдемелерді тіркеу: қазіргі жағдайы және жасанды интеллект технологияларын қолдану мәселелері — 199–203

ЛАКБАЕВ К.С., МУСИН А.Б.
Оперативно-розыскная психология: проблемы и перспективы — 204–208

МАННОНЗОДА Н.М.
Проблемы трансграничного получения цифровых доказательств при расследовании вербовки в сфере торговли людьми: уголовно-процессуальные и криминалистические проблемы (на примере Республики Таджикистан) — 209–212

МУСИН М.Ш.
Цифровой след как новый объект ОРД: Возможности и ограничения ИИ при обработке больших данных — 213–217

МУХАМЕДЖАНОВ Е.О., АПСЕТТАРОВ Р.Р.
Правовые режимы розыскной деятельности органов уголовного преследования при прерывании сроков досудебного расследования: десять лет эволюции законодательства Республики Казахстан (2016-2026) — 218–221

МУХТАРОВ Э.А.
Искусственный интеллект в предупреждении киберпреступности в Республике Казахстан: возможности, риски и перспективы — 222–228

НИЯЗАЛИЕВ Қ.А., ҚАЛМҰРАТОВ Ә.А.
Современные возможности искусственного интеллекта в выявлении синтезированной и модифицированной речи: проблемы deepfake и spoofing — 229–235

ОЛЕКСЮК М.В.
Организационно-правовые механизмы внедрения и контроля искусственного интеллекта в правоохранительной деятельности — 236–242

РАМАЗАНОВ Д.М.
Искусственный интеллект в информационно-аналитическом обеспечении противодействия преступности: возможности, риски и правовые гарантии — 243–250

САРСЕНБАЕВ О.А.
Презумпция невиновности в условиях общественного субъективизма и искусственного интеллекта: теоретико-правовой анализ — 251–257

СЫСОЕВ А.С.
Возможности искусственного интеллекта в подготовке и проведении учебных занятий по дисциплине «оперативно-розыскная деятельность органов внутренних дел» — 258–261

ХАКИМОВ Е.М., ЖУБАНДЫКОВА Л.А.
Искусственный интеллект в предпубликационной проверке официальных сообщений органов внутренних дел: правовая модель и пределы автоматизации — 262–268

ХАМЗЯЕВА Ю.Р.
Проблемы использования искусственного интеллекта в оперативно-розыскной деятельности — 269–273

ШАЛБАЕВ А.Ш.
Оперативно-розыскное прогнозирование как элемент тактического мышления в оперативно-розыскной деятельности — 274–280

ШАУДЫРОВ Т.С.
Цифровая трансформация центров оперативного управления: применение искусственного интеллекта в противодействии уголовной преступности — 281–284

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясының қорытындысы бойынша ұсынымдар 285-288

Рекомендации по итогам международной научно-практической конференции «Искусственный интеллект в противодействии преступности» 289-292

«Қылмыстылыққа қарсы іс-қимылдағы жасанды интеллект» халықаралық ғылыми-практикалық конференциясынан естелік фотолар 293