Научная статья
УДК 343
https://doi.org/10.24412/2414-3995-2025-5-29-33
EDN: https://elibrary.ru/zhqvrf
NIION: 2015-0066-5/25-332
MOSURED: 77/27-011-2025-05-531

Современные вызовы и перспективы развития оперативно-розыскной науки в условиях цифровизации

Сергей Дмитриевич Гринько
Мелитопольский государственный университет, Мелитополь, Россия,
grinko-skags@yandex.ru

Аннотация. В статье осуществляется комплексный анализ актуальных проблем и детерминант, обусловливающих необходимость трансформации оперативно-розыскной науки в контексте глобальной цифровизации. Автор акцентирует внимание на ключевых вызовах, связанных с экспансией киберпреступности, возникновением новых криминальных угроз и потребностью в адаптации оперативно-розыскной деятельности к реалиям цифровой среды. В работе критически осмысливается современный понятийно-категориальный аппарат, выявляются проблемы теоретического оснащения дисциплины, и обосновывается необходимость его обогащения новыми терминами и концептами, такими как «оперативно-розыскной мониторинг», «риск-ориентированный подход», «паспорт риска». Особое внимание уделяется методологическим аспектам интеграции передовых информационных технологий, включая искусственный интеллект, в практику оперативных подразделений. На основе анализа ведомственной статистики и тенденций криминогенной обстановки доказывается невозможность эффективного противодействия киберпреступности без развития международного полицейского сотрудничества и консолидации усилий на межгосударственном уровне. Результатом исследования является систематизация приоритетных направлений развития оперативно-розыскной науки, направленных на ее цифровую трансформацию, усиление прогностической функции и повышение эффективности обеспечения национальной безопасности в условиях цифровой реальности.

Ключевые слова: оперативно-розыскная наука, цифровизация, киберпреступность, национальная безопасность, оперативно-розыскная деятельность, искусственный интеллект, кибербезопасность

Для цитирования: Гринько С. Д. Современные вызовы и перспективы развития оперативно-розыскной науки в условиях цифровизации // Вестник экономической безопасности. 2025. № 5. С. 29–33. https://doi.org/10.24412/2414-3995-2025-5-29-33. EDN: ZHQVRF.

Original article

Modern challenges and prospects for the development of operational-search science in the context of digitalization

Sergei D. Grinko
Melitopol State University, Melitopol, Russia,
grinko-skags@yandex.ru

Abstract. This article provides a comprehensive analysis of current problems and determinants that necessitate the transformation of operational-search science in the context of global digitalization. The author focuses on key challenges related to the expansion of cybercrime, the emergence of new criminal threats, and the need to adapt operational-search activities to the realities of the digital environment. The paper critically examines the current conceptual and categorical apparatus, identifies problems in the theoretical framework of the discipline, and substantiates the need to enrich it with new terms and concepts, such as «operational and investigative monitoring», «risk-oriented approach», and «risk passport». Particular attention is paid to the methodological aspects of integrating advanced information technologies, including artificial intelligence, into the practice of operational units. Based on the analysis of departmental statistics and trends in the criminogenic situation, it is proved that effective counteraction to cybercrime is impossible without the

development of international police cooperation and the consolidation of efforts at the interstate level. The result of the research is the systematization of priority areas for the development of operational-search science, aimed at its digital transformation, strengthening of the predictive function, and improving the effectiveness of national security in the digital reality.

Keywords: operational-search science, digitalization, cybercrime, national security, operational-search activity, artificial intelligence, cybersecurity

For citation: Grinko S. D. Modern challenges and prospects for the development of operational-search science in the context of digitalization. Bulletin of economic security. 2025;(5):29–33. (In Russ.). https://doi.org/10.24412/2414-3995-2025-5-29-33. EDN: ZHQVRF.

Современный этап общественного развития, характеризующийся стремительной и тотальной цифровизацией всех сфер жизнедеятельности, детерминирует возникновение качественно новых угроз национальной безопасности. Криминальная среда, обладая значительной адаптивностью, активно осваивает цифровое пространство, порождая новые и трансформируя традиционные формы противоправных деяний. В этих условиях оперативно-розыскная наука (ОРН) как система знаний о закономерностях преступности, средствах и методах борьбы с ней оказывается перед необходимостью фундаментального переосмысления своих теоретических основ, методологического инструментария и практических ориентиров.

Актуальность темы обусловлена нарастающим разрывом между динамикой развития киберпреступности и возможностями оперативно-розыскной деятельности (ОРД) по ее своевременному выявлению, предупреждению и пресечению. Традиционные подходы, доказавшие свою эффективность в индустриальную эпоху, зачастую оказываются малорезультативными в условиях цифровой реальности, отличающейся трансграничным характером, анонимностью, высокой скоростью протекания процессов и латентностью. Следовательно, существует настоятельная потребность в научном обеспечении ОРД, адекватном вызовам современности.

Целью настоящего исследования является комплексный анализ детерминант и направлений развития оперативно-розыскной науки, направленный на преодоление существующих теоретических и практических проблем в сфере противодействия цифровой преступности. Для достижения поставленной цели необходимо решение следующих задач:

1. Выявить и систематизировать ключевые обстоятельства, обусловливающие трансформацию ОРН в условиях цифровизации.

2. Проанализировать генезис и современное состояние понятийно-категориального аппарата ОРН, определить направления его совершенствования.

3. Обосновать необходимость и перспективы внедрения риск-ориентированного подхода и системы оперативно-розыскного мониторинга в практику оперативных подразделений.

4. Оценить потенциал интеграции передовых информационных технологий, в том числе искусственного интеллекта, в оперативно-розыскной процесс.

5. Определить значение международного сотрудничества как императива в борьбе с транснациональной киберпреступностью.

Концепция развития ОРН как ответа на вызовы цифровой эпохи, а также конкретные меры по оптимизации оперативно-розыскного противодействия угрозам национальной безопасности предлагаются на основе принципа опережения.

1. Детерминанты трансформации оперативно-розыскной науки в цифровую эпоху.

Оперативно-розыскная наука переживает период глубокой трансформации, обусловленной совокупностью объективных факторов, которые формируют новую парадигму ее развития. Среди ключевых обстоятельств, оказывающих непосредственное воздействие на ее современное состояние и будущую траекторию, можно выделить следующие:

– *Четвертая промышленная революция и технологический прогресс.* Новая промышленная революция (Индустрия 4.0), основанная на киберфизических системах, интернете вещей, больших данных и искусственном интеллекте, носит необратимый характер. Она создает не только новые экономические возможности, но и уязвимости, которыми активно пользуются преступные элементы. ОРН не может оставаться в роли наблюдателя; она обязана реагировать на все вызовы цифровой среды, предлагая адекватные научно обоснованные решения [2, с. 93].

– *Глобализация и экспансия киберпреступности.* Киберпреступность приобрела характер глобального явления, не знающего национальных границ. Прогрессивное развитие цифровых технологий сопровождается возникновением и эволюцией высокоорганизованных преступных сообществ, действующих в киберпространстве. Отдельно взятое государство, как справедливо отмечают исследователи, не в состоянии самостоятельно эффективно противостоять этому вызову [1, с. 10]. Это обуславливает необходимость интернационализации предмета ОРН и активного изучения зарубежного опыта.

– *Формирование новой цифровой среды.* Правоохранительные органы вынуждены осуществлять свои функции в принципиально иных условиях – цифровой среде. Эта среда характеризуется виртуализацией, децентрализацией, изменением природы вещественных доказательств (цифровые следы), что требует разработ-

ки новых тактических приемов и методик проведения оперативно-розыскных мероприятий (ОРМ).

– *Появление новых криминальных угроз.* Цифровая среда породила ранее неизвестные формы преступной деятельности: мошенничество в сфере телекоммуникаций, отмывание денег и финансирование терроризма с использованием криптовалют, криминальный оборот в даркнете (наркотики, оружие, контрафакт), кибершпионаж, криптоджекинг и др. Опасность этих угроз многократно возрастает в связи с их масштабностью и транснациональным характером.

– *Цифровизация самой преступности.* Преступность не просто перешла в цифровую среду, она сама подверглась цифровизации, т. е. использует передовые технологии как инструмент и как среду существования. В этом смысле ОРН должна не только изучать преступность в цифровой среде, но и адекватно отвечать на технологический уровень самой преступной деятельности, находясь в состоянии непрерывной динамической адаптации и технологической трансформации.

2. Совершенствование понятийно-категориального аппарата оперативно-розыскной науки.

Одной из фундаментальных проблем, сдерживающих развитие ОРН, является отставание ее понятийно-категориального аппарата от реалий цифровой эпохи. Для объяснения процессов и явлений, происходящих в цифровой среде, необходима современная терминологическая база. Многие понятия, продиктованные новой средой, еще не получили должного теоретического осмысления в рамках предмета ОРН.

К числу таких концептов, требующих незамедлительной научной разработки и легитимации, относятся:

– *Оперативно-розыскное противодействие и его механизм.* Необходимо раскрыть сущность этого вида деятельности как целенаправленной системы мер по нейтрализации угроз национальной безопасности в цифровой среде.

– *Риск-ориентированный подход как метод ОРН.* Данный подход предполагает сосредоточение ресурсов на наиболее вероятных и опасных угрозах, их идентификацию, оценку и последующее применение адекватных мер воздействия.

– *Оперативно-розыскной мониторинг.* Под ним следует понимать непрерывное или систематическое наблюдение за состоянием криминальной обстановки в определенных сегментах цифрового пространства с целью выявления рисков и угроз на ранней стадии их возникновения.

– *«Реперные» точки оперативно-розыскного воздействия.* Это ключевые объекты, узлы или процессы в цифровой среде, воздействие на которые позволяет получить максимальный оперативный эффект.

– *«Паспорт риска».* Исследователи предлагают по результатам оперативно-розыскного мониторинга формировать «паспорт риска» – формализованный документ, который описывает конкретный объект (например, интернет-платформу, сервис), оценивает степень его криминальной пораженности и определяет необходимость и интенсивность оперативно-розыскного воздействия [2, с. 95].

Инкорпорация этих и других терминов в структуру предмета ОРН позволит не только адекватно описывать внутренние процессы науки, но и эффективно объяснять причины и характер внешнего воздействия, расширяя поле своего влияния за счет превентивных и упреждающих действий.

3. Интеграция цифровых технологий и искусственного интеллекта в оперативно-розыскную деятельность.

Цифровая трансформация ОРД является объективной необходимостью. Под цифровизацией применительно к ОРД следует понимать не просто переход на цифровую форму передачи информации, а глубинную цифровую трансформацию традиционных сил, средств, методов и форм оперативно-розыскной деятельности.

Ключевые аспекты этой трансформации включают:

– *Внедрение информационно-аналитических систем.* Использование Big Data, систем data mining и прогнозной аналитики позволяет обрабатывать огромные массивы структурированных и неструктурированных данных для выявления скрытых связей, построения поведенческих моделей преступников и прогнозирования криминальных тенденций.

– *Использование искусственного интеллекта.* Вопрос о готовности ОРН предложить практике рецепты использования ИИ для проведения отдельных ОРМ или документирования преступных действий остается открытым. Однако потенциал ИИ огромен: от автоматического анализа трафика в сетях и распознавания образов до идентификации подозрительных финансовых операций и управления роботизированными комплексами при проведении специальных операций. ОРН не должна занимать позицию догоняющей; ей необходим прорыв в этой области, требующий глубокой проработки теоретико-прикладных проблем.

– *Цифровые технологии как дискретная система.* Теоретическая модель цифровых технологий в ОРД должна быть представлена ОРН как система, основанная на способах кодирования, передачи и анализа информационных данных, позволяющая решать разнообразные оперативно-тактические задачи в сжатые временные сроки.

Разработка прикладных технологических решений для оперативных подразделений – это наукоемкий процесс, требующий консолидации усилий ученых и практиков.

4. Международное сотрудничество как императив борьбы с киберпреступностью.

Статистические данные наглядно демонстрируют масштабы проблемы. По данным МВД России, в 2022 году было зарегистрировано 318,4 тыс. киберпреступлений, что на 76,7 % больше, чем в предыду-

щем году. Более половины из них (57,3 %) совершены с использованием сети «Интернет», а свыше трети (42,7 %) – посредством мобильной связи. Особенно резко возросло число преступлений с использованием расчетных карт – в 5 раз [5].

Эти цифры подтверждают глобальный характер угрозы. Повышения эффективности борьбы с киберпреступностью можно добиться лишь путем объединения усилий правоохранительных органов на международном уровне. Ключевыми составляющими такого сотрудничества являются:

– *Гармонизация законодательства.* Активная работа под эгидой ООН по выработке международной Конвенции о борьбе с киберпреступностью является насущной необходимостью.

– *Оперативный обмен информацией.* Создание каналов быстрого и защищенного обмена оперативно-значимой информацией между правоохранительными органами разных стран.

– *Проведение совместных операций.* Организация и проведение скоординированных транснациональных оперативно-розыскных операций.

Эти вопросы должны стать объектом пристального внимания ОРН и войти в ее предмет как неотъемлемый элемент системы знаний о противодействии современной преступности.

5. Методологические ориентиры и стратегическое планирование.

Успешное методологическое перевооружение ОРН должно осуществляться в соответствии с основными положениями Концепции научно-технической политики МВД России до 2030 года [4]. Одним из ключевых принципов данной Концепции является интеграция ведомственной науки, образования и практики. Среди ее приоритетов – выявление, пресечение, раскрытие и расследование преступлений, в том числе посредством развития ОРД и экспертно-криминалистической деятельности.

В этом контексте важным методологическим направлением является также снижение административного давления на бизнес со стороны правоохранительных органов [3, с. 42]. Разработка научных основ для дифференциации подхода к субъектам предпринимательства, недопущения необоснованного вмешательства в их деятельность при одновременном обеспечении эффективного контроля, требует дальнейших теоретических исследований.

ОРН свойственны прогнозирование и стратегическое планирование. В связи с этим назрела необходимость в разработке отдельной Стратегии внедрения информационных технологий в оперативно-розыскную деятельность. Такой документ определил бы четкие цели, этапы и ожидаемые результаты цифровой трансформации ОРД, задав тем самым вектор движения для всей оперативно-розыскной науки.

Проведенное исследование позволяет сформулировать следующие выводы и предложения.

1. Оперативно-розыскная наука находится под определяющим влиянием цифровизации. Это влияние проявляется в необходимости адекватного ответа на новые технологические вызовы, адаптации к цифровой среде и трансформации собственного методологического аппарата. Ответом ОРН на коренные преобразования в системе информационных технологий стало внедрение в деятельность оперативных подразделений информационно-поисковых систем, автоматизированных банков данных и электронного документооборота.

2. Ключевым процессом является цифровая трансформация ОРД. Это не просто техническое перевооружение, а фундаментальное изменение традиционных сил, средств, методов и форм оперативно-розыскной деятельности, результатом которого станет представление всего оперативно-розыскного процесса в конечной, цифровой форме, пригодной для автоматизированного анализа и управления.

3. Необходимо срочное обновление понятийно-категориального аппарата ОРН. Введение и легитимация таких понятий, как «оперативно-розыскной мониторинг», «риск-ориентированный подход» и «паспорт риска», позволят науке адекватно описывать и объяснять реалии цифровой эпохи и выстраивать на этой основе эффективные модели противодействия.

4. Интеграция искусственного интеллекта и передовых аналитических систем – это стратегический императив. ОРН должна стать локомотивом внедрения данных технологий, предложив практикам научно обоснованные алгоритмы и методики их применения для решения оперативно-тактических задач.

5. Развитие международного полицейского сотрудничества является обязательным условием эффективного противодействия транснациональной киберпреступности. ОРН призвана разрабатывать теоретические основы и практические механизмы такого сотрудничества.

Таким образом, дальнейшее развитие оперативно-розыскной науки видится в ее способности к самообновлению, активной интеграции междисциплинарных знаний, опережающему прогнозированию угроз и формированию на этой основе научного фундамента для эффективного обеспечения национальной безопасности Российской Федерации в XXI веке.

Список источников

1. Жданов Ю. Н., Овчинский В. С. Киберполиция XXI века : международный опыт. М. : Юрайт, 2020. 285 с.

2. Иванов П. И. Цифровая реальность и ее влияние на развитие оперативно-розыскной науки // Цифровые технологии в борьбе с преступностью : проблемы, состояние, тенденции : сб. науч. ст. М. : Проспект, 2021. С. 92–100.

3. Иванов П. И., Шитов А. С. Уголовная политика в области борьбы с налоговой преступностью и особенности ее реализации подразделениями экономической

безопасности и противодействия коррупции органов внутренних дел Российской Федерации // Уголовная политика и культура противодействия преступности : матлы междунар. науч.-практ. конф. Краснодар : КубГАУ, 2020. С. 40–46.

4. Концепция научно-технической политики МВД России до 2030 года (Основные положения). М. : ФГКОУ ВО «Академия управления МВД России», 2019. 56 с.

5. Письмо Следственного департамента МВД России от 5 октября 2022 г. № 17/3-34272 «О направлении алгоритма действий следователя на первоначальном этапе расследования дистанционных хищений» // СПС «КонсультантПлюс».

References

1. Zhdanov Yu. N., Ovchinsky V. S. Cyberpolice of the XXI century : international experience. M. : Yurait, 2020. 285 p .

2. Ivanov P. I. Digital reality and its impact on the development of operational investigative science // Digital technologies in the fight against crime : problems, status, trends : collection of scientific articles. M. : Prospekt, 2021. P. 92–100.

3. Ivanov P. I., Shitov A. S. Criminal policy in the field of combating tax crime and the specifics of its implementation by economic security and anti-corruption units of the internal affairs bodies of the Russian Federation // Criminal policy and culture of crime prevention : materials of the international scientific and practical conference. Krasnodar : KubGAU Publ., 2020. P. 40–46.

4. The concept of scientific and technical policy of the Ministry of Internal Affairs of Russia until 2030 (Main provisions). M. : FGKOU HE «Academy of Management of the Ministry of Internal Affairs of Russia», 2019. 56 p.

5. Letter from the Investigative Department of the Ministry of Internal Affairs of Russia dated October 5, 2022 № 17/3-34272 «On the direction of the investigator's algorithm of actions at the initial stage of the investigation of remote theft» // LRS «ConsultantPlus».

Информация об авторе

С. Д. Гринько – заведующий кафедрой уголовно-правовых дисциплин Мелитопольского государственного университета, кандидат юридических наук, доцент.

Information about the author

S. D. Grinko – Head of the Department of Criminal Law Disciplines of the Melitopol State University, Candidate of Legal Sciences, Associate Professor.

Статья поступила в редакцию 08.09.2025; одобрена после рецензирования 24.09.2025; принята к публикации 10.10.2025.

The article was submitted 08.09.2025; approved after reviewing 24.09.2025; accepted for publication 10.10.2025.