УДК 34

Теоретические и практические аспекты совершенствования оперативно-розыскной деятельности в условиях цифровой трансформации современного общества

Демченко Виктория Викторовна

Кандидат юридических наук, доцент,
подполковник полиции,
кафедра оперативно-розыскной деятельности и специальной техники,
Луганский филиал Воронежского института МВД России,
91000, Российская Федерация, Луганск, ул. Щаденко, 20а;
e-mail: vika.dvv77@yandex.ru

Аннотация

Цифровая трансформация современного общества предъявляет новые требования к оперативно-розыскной деятельности (ОРД), вынуждая правоохранительные органы адаптировать традиционные методы к реалиям киберпространства. Статья исследует комплексный подход к модернизации ОРД, включающий внедрение инновационных технологий для сбора и анализа больших данных, мониторинга сетевой активности и выявления преступных схем с помощью алгоритмов искусственного интеллекта. Особое внимание уделяется необходимости развития вычислительной инфраструктуры, аналитических платформ и систем кибербезопасности для защиты конфиденциальной информации от несанкционированного доступа. Автор подчеркивает важность непрерывного повышения квалификации оперативного состава, включая освоение методов киберразведки, анализа сетевых протоколов и криптографии, что является критическим фактором эффективности в условиях динамично развивающихся угроз. Параллельно исследуются правовые и этические вызовы, связанные с цифровизацией ОРД. Обсуждается необходимость баланса между оперативной эффективностью и соблюдением прав граждан, включая защиту персональных данных и приватности коммуникаций. Статья акцентирует важность формирования четких правовых механизмов и международных стандартов для регулирования сбора цифровых доказательств, трансграничного обмена информацией и предотвращения злоупотреблений. Рассматриваются риски алгоритмических ошибок, ложных срабатываний систем анализа данных и этические дилеммы массового мониторинга. Подчеркивается роль прозрачности правоприменения и взаимодействия с гражданским обществом для сохранения доверия к правоохранительным органам. В заключении обосновывается тезис о том, что успешная цифровая трансформация ОРД возможна только при интеграции технологических инноваций с традиционными методами оперативной работы, развитии межведомственного и международного сотрудничества, а также создании надежных правовых гарантий. Ключевым условием названо сохранение принципа "человек в центре принятия решений" для минимизации рисков автоматизированных систем и обеспечения соответствия деятельности демократическим ценностям.

Для цитирования в научных исследованиях

Демченко В.В. Теоретические и практические аспекты совершенствования оперативно-розыскной деятельности в условиях цифровой трансформации современного общества // Вопросы российского и международного права. 2025. Том 15. № 4А. С. 345-356.

Ключевые слова

Цифровая трансформация, оперативно-розыскная деятельность, кибербезопасность, большие данные, правовое регулирование.

Введение

Современное общество переживает период глубокой цифровой трансформации, которая затрагивает практически все аспекты человеческой деятельности. Развитие информационных технологий и повсеместное распространение сети Интернет способствуют не только ускорению обмена данными, но и коренному изменению способов коммуникации и получения информации. В сфере оперативно-розыскной деятельности эти процессы вызывают необходимость пересмотра устоявшихся подходов, так как преступные элементы активно используют новые инструменты цифрового пространства для сокрытия своей деятельности. Возникает объективное требование к формированию новых методик и технологий секретного наблюдения, внедрения инновационных средств сбора и анализа данных, а также активизации межведомственного взаимодействия в онлайновой среде. При этом важно учитывать тот факт, что цифровая трансформация меняет не только технические методы, но и само содержание повседневной деятельности оперативных подразделений, вынуждая обеспечивать высокий уровень квалификации сотрудников. Однако практика показывает, что универсального решения не существует, и каждая правоохранительная структура пытается адаптироваться под новые угрозы по-своему. Важно также помнить о рисках, связанных с ростом объемов собираемой информации, ведь большие данные требуют соответствующей системы хранения и обработки. Не последнее место занимает кибербезопасность, обеспечивающая защиту аналитических платформ и сервисов от несанкционированного вмешательства. Ошибки на уровне электронных баз могут привести к системным сбоям, и тогда эффективность оперативной работы будет подорвана. Разумная модернизация, сочетание проверенных временем методов и технологий машинного обучения позволяют повысить результативность выявления и пресечения правонарушений. Главная задача при этом – не только отреагировать на уже совершенные преступления, но и предвидеть возможные угрозы, предотвращая преступные замыслы на этапе их возникновения. Актуальность вопроса усугубляется и тем, что цифровая трансформация устанавливает новое понимание секретности, поскольку цифровые следы могут быть извлечены и проанализированы значительно быстрее, чем традиционные физические доказательства. [Бабушкин, 2020] Техническая грамотность персонала становится залогом быстроты собирания улик и повышения качества доказательной базы, однако дальнейшее развитие технологий требует еще более пристального внимания к вопросам правового регулирования их использования.

Основное содержание

С теоретической точки зрения, модернизация оперативно-розыскной деятельности в условиях цифровой трансформации подразумевает необходимость комплексного пересмотра методологических положений, лежащих в основе поиска оперативно значимой информации. [Туркаева, 2020] Традиционный подход, основанный на оперативном наблюдении, агентурной работе и физическом контроле территории, дополняется инструментами, позволяющими отслеживать перемещения в цифровом пространстве, анализировать сетевую активность потенциальных правонарушителей и формировать банк данных типовых схем преступной деятельности. Это связано также с внедрением аналитических алгоритмов, способных обнаруживать скрытые связи между лицами и событиями, которые на первый взгляд не имеют ничего общего. [Тороп, 2023] Использование таких интеллектуальных систем существенно ускоряет рутинные процессы, освобождая специалистов от тяжелой аналитической работы и позволяя сосредоточиться на разработке стратегических мер пресечения организованной преступности. При этом возникает парадоксальная ситуация: чем сложнее становятся инструменты анализа, тем выше риск неправильной интерпретации данных или использования неполной информации. Если при традиционных способах оперативной работы все зависит от человеческого фактора, то при эксплуатации цифровых систем фактором риска становятся алгоритмические ошибки, неадекватные значения весовых коэффициентов и статистические выбросы в выборках. Это, конечно, не отменяет важности участия человека, ведь по-прежнему требуется экспертное мнение по сложным вопросам, связанным с оценкой достоверности выводов алгоритма. Но важность автоматизации настолько велика, что формируется устойчивый тренд на расширение спектра цифровых инструментов, используемых правоохранительными органами во всем мире.

Материалы и методы исследования

Одновременно необходимо обеспечить должный уровень правовых механизмов, регламентирующих использование подобных средств анализа, ведь недопустимо, чтобы расширение полномочий оперативных подразделений превратилось в нарушение прав граждан. [Искалиев, 2023] Правовая защита персональных данных, свобода слова и тайна частной коммуникации – ключевые понятия, которые современные государства стремятся балансировать с потребностями обеспечения общественной безопасности. Особую роль играют международные соглашения, определяющие порядок доступа к электронным доказательствам и трансграничного обмена информацией о преступной деятельности. Это требует координации между различными юрисдикциями, выработки единых стандартов безопасности и унификации процедур выявления, сбора и верификации улик, полученных в цифровом формате. [Ткачук, Курысев, 2023] При этом каждая страна стремится не только следовать общей глобальной практике, но и устанавливать собственные правовые нормы, что порождает несостыкованности и сложности при расследовании дел, охватывающих несколько государств. Поэтому в рамках развития оперативно-розыскной деятельности становится необходимым межнациональное сотрудничество, создание объединенных баз данных, регулярные обмены экспертным опытом и формирование единых подходов к киберугрозам. Значимость этого аспекта возрастает с каждым годом, ведь преступление в киберпространстве не знает границ, и преступники могут использовать юрисдикционные пробелы или отсутствие согласованного законодательства для

уклонения от правосудия.

Практическая реализация идей цифровой трансформации оперативно-розыскной деятельности предполагает внедрение как технологических, так и организационных инноваций. [Яковец, 2020] С одной стороны, это развитие вычислительной инфраструктуры, аналитических центров и программных комплексов, способных обрабатывать большие массивы данных в режиме реального времени. С другой стороны, важен и кадровый аспект: повышение квалификации сотрудников, формирование внутриорганизационных образовательных программ, обучающих современным методам кибер разведки и анализа сетевых коммуникаций. В итоге на первый план выходит комплексный подход к обучению оперативного состава, включающий не только теоретические курсы по криминалистике, но и практикум по работе с цифровыми платформами мониторинга. [Агеенков, Ефанов, 2020] Важно, что обновление кадрового потенциала становится практически непрерывным процессом, ведь развитие технологий, появление новых преступных схем и совершенствование инструментов сокрытия следов вынуждают специалистов постоянно повышать уровень знаний. Опираясь на опыт стран, активно ведущих кибероперации, можно сказать, что без постоянного пополнения теоретических и практических навыков невозможно эффективно противостоять динамичным угрозам XXI века. Технологическая сторона вопроса требует внедрения комплексных систем, способных не только собирать и хранить информацию, но и осуществлять углубленный анализ связей, определять закономерности и предсказывать возможные сценарии развития событий.

Результаты и обсуждение

На этом фоне актуальным становится вопрос о стандартизации и сертификации используемых инструментов, поскольку неконтролируемое применение разнообразных программ и аппаратных комплексов может привести к методологическим ошибкам, несовместимости данных и затруднить их совместный анализ. [Иванов, 2024] Одно дело – внедрить отдельную программу для сбора информационных следов, и совсем другое – создать целостную систему, включающую в себя аппаратные модули перехвата и декодирования цифрового трафика, распределенные аналитические платформы, средства защиты от несанкционированного доступа, а также межведомственные каналы обмена информацией. В условиях, когда любая ошибка может привести к утечке данных или дискредитации доказательств в суде, крайне важно наличие четко прописанных протоколов работы. [Тимофеев, 2024] Такими протоколами могут выступать как внутренние ведомственные инструкции, так и национальные стандарты, а иногда и международные руководства по обращению с цифровыми доказательствами. Формирование такой нормативно-методической базы обретает ключевое значение, так как оперативные подразделения могут взаимодействовать не только с коллегами по другим регионам внутри страны, но и с экспертами за рубежом, которому тоже необходимо передавать и получать информацию в рамках официальных процедур.

При этом цифровая трансформация несет в себе и новые вызовы, одним из которых является обеспечение кибербезопасности самих правоохранительных органов. Информационные системы, которые принимаются на вооружение, могут стать целью атак со стороны преступных структур или хакерских группировок, стремящихся получить доступ к служебным базам, изменить или удалить важные сведения. [Семенчук, Батоев, 2023] Кроме того, существует угроза дискредитации данных через преднамеренное внесение искаженной информации, что может поставить под сомнение достоверность всей системы. Поэтому в число приоритетных

направлений деятельности входит разработка и поддержание надежной архитектуры защиты, включающей антивирусные решения, системы обнаружения вторжений, регулярные аудиты безопасности, обучение персонала принципам кибергигиены. В то же время не стоит абсолютно полагаться на технические меры: человеческий фактор по-прежнему может приводить к ошибкам, когда сотрудники своей небрежностью или умышленными действиями открывают доступ к конфиденциальным ресурсам. [Еркалов, 2022] Практика многих стран показывает, что грамотное управление доступами, многоуровневая аутентификация и строгий контроль за действиями персонала являются важнейшими элементами защиты внутренних сетей оперативных подразделений.

Отдельного внимания заслуживает вопрос этического характера, а именно баланс между эффективностью оперативно-розыскной деятельности и соблюдением прав человека в цифровой среде. Чем более развиты технические возможности контроля, тем выше вероятность вмешательства в частную жизнь граждан, когда сбор данных происходит в массовом порядке. [Щетнёв, 2023] В некоторых случаях использование тотального мониторинга может дать действительно впечатляющие результаты по выявлению криминальных структур, однако общество справедливо высказывает опасения по поводу возможного злоупотребления такими технологиями. Отсюда следует, что правовое регулирование этой сферы и наличие механизмов надзора должны быть прозрачными и понятными широкой публике, чтобы не формировалось ложное впечатление о “тотальной слежке” за населением. Современный цивилизованный подход к оперативно-розыскной деятельности в цифровую эпоху предполагает тесное взаимодействие с институтами гражданского общества, правозащитными организациями и СМИ, что позволяет поддерживать доверие к правоохранительным органам. [Иванов, 2022] Если это доверие будет подорвано, то общество станет относиться к представителям закона с подозрением, а преступники, напротив, смогут убедить людей в несправедливости существующих порядков, тем самым получая негласную поддержку скрывающейся в цифровом пространстве оппозиции.

Опираясь на положительный опыт ряда государств, можно отметить, что эффективное использование цифровых технологий в оперативно-розыскной деятельности требует не только технического оснащения, но и выработки методической культуры работы с информацией. Аналитик, работающий с большими данными, должен понимать их ограничения, критически относиться к результатам автоматизированных алгоритмов, уметь выявлять и искаженные данные, и двойные учетные записи. Но даже высокого уровня профессионализма мало, если сама система не позволяет оперативно задействовать результаты аналитики в реальной практике. Нужна отлаженная структура управления, где орган, занимающийся сбором информации, эффективно взаимодействует с подразделением, отвечающим за принятие решений и реализацию конкретных оперативных мер. [Семенчук, Батоев, 2023] Без такого разделения компетенций и без четкой регламентации процессов трудно рассчитывать на высокую результативность. При этом скорость принятия решений в цифровую эпоху играет ключевую роль, так как преступники могут действовать в режиме реального времени, быстро меняя тактику и места дислокации.

Вместе с тем расширяется список специальных знаний, необходимых для оперативных работников и криминалистов, занимающихся расследованием электронной преступности. Постепенно возрастает роль специалистов, владеющих навыками программирования, криптографии, анализа сетевых протоколов и методов обнаружения вредоносных программ. [Белый, Сурцев, 2020] Создание аналитических порталов, способных визуализировать сложные

взаимосвязи между объектами, дополняется внедрением механизмов искусственного интеллекта, которые на базе больших данных позволяют выявлять аномальные паттерны в поведении пользователей. Такие алгоритмы эффективно работают на больших платформах, но требуют значительных вычислительных ресурсов и сложного сопровождения. Подобные решения, даже будучи весьма дорогостоящими, оправдывают себя, когда ловля преступников идет буквально по горячим цифровым следам, и время на установление фактов имеет решающее значение. Кроме того, есть направления дальнейшей интеграции такие, как использование блокчейн-технологий для гарантии неизменности собранных доказательств или применение распределенных реестров для организации безопасного обмена информацией между разными ведомствами.

Нельзя упускать из виду и проблемы, связанные с масштабированием цифровых решений. Когда речь идет о локальных киберподразделениях, где работают единицы или десятки специалистов, оптимизация относительно проста. Но когда правоохранительная структура включает в себя тысячи сотрудников, разбросанных по всей стране, интеграция цифровых систем может затянуться на годы, и только профессиональное проектное управление способно скоординировать все этапы внедрения. При этом важно, чтобы выбранные решения не устарели морально по мере их внедрения, ведь технологический прогресс очень скоротечен. [Туркаева, 2020] Организации часто сталкиваются с ситуацией, когда завершают установку и тестирование программного комплекса, а на рынке уже появились более совершенные версии или совершенно новые подходы к решению тех же задач. Попытки “догнать” развитие рынка технологий постоянно создают необходимость проводить апгрейд оборудования, тратиться на обучение персонала, пересматривать внутренние инструкции и менять подход к обработке данных. Неудивительно, что некоторые правоохранительные органы стараются выбирать решения по модульному принципу, позволяющему гибко наращивать функциональность без полной перестройки систем.

Помимо технических нюансов, вырисовывается проблема правоприменительной практики, где суды, прокуратура и адвокаты должны уметь работать с цифровыми доказательствами. Применение крупных аналитических платформ в оперативно-розыскной деятельности может быть сведено на нет, если суд не примет электронные данные в качестве надлежащего доказательства или если будет оспорено соблюдение процедуры их получения. [Ткачук, Курысев, 2023] Поэтому формирование правовых процедур, детализирующих порядок сбора, фиксации, сохранения и предоставления сведений цифрового характера, играет не меньшую роль, чем сама технология. Юридические эксперты вместе с айти-специалистами разрабатывают стандарты, призванные сделать работу с цифровыми носителями надлежащей с точки зрения защиты прав и свобод граждан. Судебная система, в свою очередь, постепенно адаптируется к тому, что все чаще приходится исследовать айпи-адреса, логи серверов, результаты экспертиз вредоносного кода. [Искалиев, 2023] Остается вопрос: какие факторы могут поколебать правдивость таких доказательств, ведь киберсреда позволяет вносить незаметные модификации в данные, удалять записи и искажать временные метки.

Эффективное противостояние киберпреступникам складывается из множества компонентов, и одним из наиболее важных среди них является международная кооперация. Несмотря на то что цифровая трансформация существенно облегчает обмен информацией, межгосударственные барьеры по-прежнему остаются достаточно высокими. Каждый государственный орган руководствуется собственными процедурами, а договорённости между странами требуют сложных дипломатических усилий. [Тимофеев, 2024] К тому же, когда речь

идет о пресечении преступности в интернете, важно учитывать, что сервера и провайдеры могут располагаться в разных уголках мира, часто в юрисдикциях с разными законодательными нормами и интересами. Преступники умело пользуются этим обстоятельством, пряча свои операции за границей, выбирая страны с неразвитым законодательством или отсутствием специальных соглашений о передаче подозреваемых. В ответ на это правоохранительные органы пытаются формировать международные рабочие группы, проводить совместные спецоперации, а также содействовать обмену данными о подозреваемых лицах и технологических схемах преступлений. Опыт показывает, что это весьма сложный процесс, требующий от оперативных сотрудников знаний не только национального, но и международного права.

В быстрых темпах модернизации оперативно-розыскной деятельности важно сохранить преемственность традиционных методов, которые доказали свою эффективность на протяжении многих лет практики. [Тороп, 2023] Агентурная работа, наблюдение, проверка личности, опрос свидетелей – все это не теряет свою актуальность, а зачастую оказывается решающим фактором в установлении истины. Цифровые инструменты – не панацея, а лишь мощное дополнение к тем формам оперативной деятельности, которые зарекомендовали себя в разных странах мира. Однако происходит взаимопроникновение методов: сведения, полученные из агентурных источников, могут послужить исходными данными для цифрового анализа, а результаты кибермониторинга – подсказать направление для проведения классических мероприятий. Баланс между традицией и инновацией – это то, чего следует добиваться правоохранительным органам в условиях глобальных изменений, где цифровые каналы коммуникации становятся доминирующими, но человеческий фактор все еще играет ключевую роль.

В тех случаях, когда анализ больших массивов данных позволяет выявить потенциальные угрозы, возникает вопрос о том, как выстроить превентивную работу, не нарушая при этом прав отдельных граждан, попавших в подозрение из-за статистических корреляций. [Белый, Сурцев, 2020] Алгоритмы машинного обучения могут выдавать ложные срабатывания, и если не обеспечить адекватный механизм проверки, то в поле зрения оперативных органов могут оказаться невиновные люди. Это требует от разработчиков и заказчиков аналитических систем более тщательной настройки алгоритмов, регулярной проверки их корректности и прозрачного механизма апелляции к результатам, полученным автоматически. Именно концепция “человек в центре принятия решений” призвана ярузно уравновешивать технологическую готовность и социоправовые ограничения. Важно понимать, что использовать искусственный интеллект и другие цифровые инструменты нужно именно в интересах общества, а не для безосновательного вторжения в личную жизнь.

Вместе с тем цифровая трансформация может стать стимулом к усилению кадрового потенциала не только оперативно-розыскной сферы, но и смежных отраслей криминалистики, судебной экспертизы, а также научно-исследовательских работ. Совместные проекты университетов, следственных органов и частных IT-компаний способны обеспечить необходимый научный фундамент, способствовать изобретению новых технологий поиска и анализа цифровых следов. [Семенчук, Батоев, 2023] Практика показывает, что иногда именно частные компании разрабатывают наиболее передовые решения в области кибербезопасности, а правоохранительные органы, сотрудничая с ними, получают бесценные инструменты для обнаружения и документирования криминальных схем. При этом государство должно формировать и стимулировать такие коллаборации, обеспечивать финансирование и правовые

условия для проведения крупных научно-производственных экспериментов, направленных на совершенствование оперативно-розыскной деятельности.

Рост террористических угроз и экстремизма также меняет задачу оперативных подразделений, вынуждая их ориентироваться на превентивную аналитику, способную выделить в огромном потоке сетевых коммуникаций радикальные идеи и группы, склонные к противоправным действиям. [Щетнёв, 2023] Цифровая трансформация, с одной стороны, помогает правоохранителям своевременно выявлять такие группы, отслеживать динамику их вербовки и каналы финансирования. С другой стороны, злоумышленники быстро адаптируются, уходя в зашифрованные мессенджеры или темную сеть, где создают закрытые сообщества. Поэтому технологии, необходимые для оперативного контроля такой среды, требуют высокого профессионализма и наличия специальных программно-аппаратных комплексов. Есть и сложный вопрос определения границ свободы слова, чтобы не преследовать гражданскую активность, не связанную с реальной угрозой безопасности. В этом плане вопрос цифровой трансформации выходит за рамки чисто технических решений, становясь предметом общественно-политических дискуссий и формируя новые нравственные императивы.

Подход к оперативно-розыскной деятельности, основанный на глубоком анализе сложных информационных потоков, вынуждает уделять особое внимание простоте и удобству пользовательских интерфейсов, с которыми ежедневно работают оперативники. Если аналитические платформы будут перегружены технически сложными модулями и не будут иметь адаптированного под нужды практиков интерфейса, то эффект от их применения может оказаться ниже ожидаемого. [Яковец, 2020] Это особенно ярко проявляется в крупных ведомствах, где масса сотрудников имеет разные уровни владения компьютером, разный опыт участия в цифровых проектах и неодинаковое восприятие нововведений. Постоянное совершенствование интерфейса и функционала должно сопровождаться обучающими программами, максимально доступными и понятными, чтобы сотрудники не тратили время на поиск базовых функций, а могли сосредоточиться на анализе сути дела. В идеале, современные системы должны уметь работать на разных устройствах, в том числе мобильных, потому что оперативники часто находятся в разъездах, на местах происшествий или в режимах скрытого наблюдения, где удобнее использовать планшет или специализированный мобильный терминал.

Важный аспект совершенствования оперативно-розыскного процесса – это формирование единой базы знаний, содержащей статистические материалы о преступных схемах, методах сокрытия улик, особенностях различных преступных группировок. [Агеенков, Ефанов, 2020] В условиях цифровизации такую базу выгоднее хранить в облачной среде с высоким уровнем защиты и оперативным доступом для уполномоченных сотрудников. Тогда при возникновении похожих кейсов оперативники смогут быстрее находить аналоги, сравнивать ключевые факторы и переносить удачные практики на новые случаи. Интеграция этой базы с аналитическими модулями позволит в полуавтоматическом режиме выдвигать гипотезы о возможном развитии ситуации и даже предлагать рекомендации по способам нейтрализации угрозы. Однако для успешного функционирования такой системы нужны четкие правила внесения и обновления информации, регулярные аудиты и контроль за репутационными рисками, ведь в единую базу могут попасть ошибочные или намеренно ложные сведения.

При всей сложности цифровой перестройки системы оперативно-розыскной деятельности можно говорить о том, что в перспективе она способна радикально повысить прозрачность и надежность привлечения к ответственности преступников. Цифровые следы, которые

оставляют преступники в Интернете, зачастую более обстоятельны, чем следы реальной деятельности, поскольку могут содержать временные метки, геолокацию, записи коммуникаций и платежей. [Семенчук, Батоев, 2023] При правильном подходе к обеспечению аутентичности и соблюдению процессуальных норм эти цифровые улики могут служить весьма надежной базой для судебного преследования, в том числе в международном формате. Но следует помнить, что преступники также пытаются использовать цифровые возможности, как то подделка данных, внедрение вирусов в чужие системы или распространение дезинформации. Постоянная конкуренция "меча и щита" в цифровом пространстве стимулирует развитие еще более совершенных систем защиты и анализа.

Значимым является и вопрос распределения ответственности между государственными ведомствами, частными компаниями и гражданским обществом. Цифровая трансформация оперативно-розыскной деятельности часто требует доступ к данным, которые находятся на коммерческих серверах, принадлежат интернет-провайдерам или социальным платформам. [8] Поэтому отлаженные механизмы взаимодействия государства и бизнеса, основанные на четких правовых нормах, являются критическим элементом эффективной борьбы с преступностью. Без согласия и готовности коммерческих структур сотрудничать в законных рамках государственные органы могут не получить нужных сведений в нужные сроки. С другой стороны, бизнес должен быть уверен, что не нарушает права своих пользователей и не несет репутационных потерь, сотрудничая с властями. От этого зависит и доверие клиентов к сервисам, которые, в свою очередь, стремятся обеспечивать конфиденциальность данных. В результате получается тонкое поле взаимодействия, где каждая сторона имеет собственные интересы, и все они должны быть сбалансированы так, чтобы сохранять и конституционные свободы, и эффективность работы оперативных служб.

Виртуальное пространство способствует развитию сетевых криминальных сообществ, что значительно усложняет задачу поиска лидеров этих группировок и доказывания их вины. [Иванов, 2022] Часто преступная сеть децентрализована, не имеет ярко выраженной структуры, а ее члены могут находиться в разных точках земного шара. В таких случаях традиционные методы оперативной работы оказываются недостаточными, и приходится внедрять многоступенчатый комплекс мер, включающих тайное внедрение агентов в электронные сообщества, криптоанализ зашифрованных сообщений, мониторинг платежей в крипто валютах. При этом важно вести многостороннюю координацию, ведь любая утечка или задержка в одном звене может привести к провалу всей операции, а преступники, заметив повышенное внимание, мгновенно поменяют каналы коммуникаций.

Заключение

Наконец, в условиях цифровой трансформации растет роль публичных источников информации, включая социальные сети, блоги, форумы и новостные порталы. [Иванов, 2024] Анализ открытых данных может предоставить правоохранительным органам ценные сведения о настроениях в обществе, о признаках планируемых протестных акций, о вероятных участниках конфликтных ситуаций. Это особенно полезно при мониторинге экстремистских проявлений, пропаганды насилия или вербовки в закрытые сообщества. Однако существует и опасность переоценки значимости таких данных, ведь недостоверная информация или троллинг могут вводить анализ в заблуждение. Чтобы компенсировать эти риски, оперативники должны владеть навыками критического отбора и верификации получаемых сведений, использовать машинное обучение для фильтрации ложного контента, но непременно проверять полученное в

ходе ручного анализа.

В итоге становится очевидно, что процесс совершенствования оперативно-розыскной деятельности в эпоху цифровой трансформации общества – это комплексная и многоплановая задача. Она включает техническую, организационную, правовую, кадровую и этическую составляющие, каждая из которых вносит вклад в конечную эффективность. [Туркаева, 2020] Ключевым моментом остается грамотное сочетание традиционных методов оперативной работы с новейшими цифровыми инструментами. Без фундаментальной подготовки, без поддержки государства на высшем уровне, без инноваций, исходящих из научной среды и частного сектора, достичь успеха в противостоянии современной преступности невозможно. Цифровая трансформация объективна и необратима, она открывает новые горизонты в сфере оперативно-розыскной деятельности, позволяя использовать передовые методы анализа данных и расширять возможности правоохранительных органов. Но только при четком соблюдении прав и свобод человека, при открытом взаимодействии с общественностью и международными партнерами, а также при непрерывном обновлении компетенций специалисты смогут эффективно отвечать на вызовы криминального мира, не теряя доверия граждан и не допуская учреждения тотального контроля над личной жизнью.

Библиография

1. Семенчук В.В., Батоев В.Б. Предпосылки формирования концепции развития оперативно-разыскной деятельности в цифровой сфере (часть 1) // Вестник Волгоградской академии МВД России. 2023. № 3 (66). С. 132-136.
2. Ткачук Т.А., Курысев К.Н. Вопросы о децифровизации в аспекте осуществления оперативно-разыскной деятельности // Вестник Владимирского юридического института. 2023. № 1 (66). С. 107-111.
3. Агеенков А.А., Ефанов С.И. Об отдельных проблемах осуществления оперативно-разыскной деятельности в современных условиях // Вестник Рязанского филиала Московского университета МВД России. 2020. № 14. С. 30-37.
4. Тороп С.С. Цифровые возможности в оперативно-разыскной деятельности // Вестник молодых ученых Самарского государственного экономического университета. 2023. № 1 (47). С. 122-126.
5. Тимофеев С.В. Современные доминанты в оперативно-разыскной деятельности // Философия права. 2024. № 2 (109). С. 180-186.
6. Иванов П.И. Оперативно-разыскная деятельность в условиях цифровой реальности: её научное обеспечение // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2022. № 2 (68). С. 64-67.
7. Туркаева Л.В. Правовая сущность оперативно-разыскной деятельности органов внутренних дел и её значение в борьбе с преступностью // Правопорядок: история, теория, практика. 2020. № 4 (27). С. 66-70.
8. Еркалов А.А. Правоприменение и акты правоприменения в оперативно-разыскной деятельности // Юридическая наука. 2022. № 6. С. 91-96.
9. Искалиев Р.Г. Совершенствование методов оперативно-разыскной деятельности в современных условиях цифровой трансформации // Закон и право. 2023. № 12. С. 201-207.
10. Семенчук В.В., Батоев В.Б. Предпосылки формирования концепции развития оперативно-разыскной деятельности в цифровой сфере (часть 2) // Вестник Волгоградской академии МВД России. 2023. № 4 (67). С. 165-174.
11. Щетнёв Л.Е. Правовые и теоретические подходы к сущности оперативно-разыскного мероприятия "Оперативное внедрение" // Вестник Владимирского юридического института. 2023. № 1 (66). С. 112-115.
12. Бабушкин В.А. Законодательные основы проведения органами внутренних дел мероприятий в сфере оперативно-разыскной аналитики // Российский следователь. 2020. № 12. С. 60-64.
13. Яковец Е.Н. Некоторые актуальные проблемы теории и практики оперативно-разыскной деятельности // Эпомен. 2020. № 40. С. 293-313.
14. Белый А.Г., Сурцев А.В. Современные представления о системе и принципах оперативно-разыскной деятельности // Евразийский юридический журнал. 2020. № 8 (147). С. 264-265.
15. Иванов П.И. Оперативно-разыскное сопровождение расследования преступлений: понятие, сущность и содержание // Вестник Владимирского юридического института. 2024. № 2 (71). С. 32-35.

Theoretical and Practical Aspects of Improving Investigative Activities in the Context of Digital Transformation of Modern Society

Viktoriya V. Demchenko

PhD in Law, Associate Professor,
Police Lieutenant Colonel,
Department of Investigative Activities and Special Equipment,
Lugansk Branch of the Voronezh Institute of the Russian Ministry of Internal Affairs,
91000, 20a Shchadenko str., Lugansk, Russian Federation;
e-mail: vika.dvv77@yandex.ru

Abstract

The digital transformation of modern society imposes new requirements on investigative activities, compelling law enforcement agencies to adapt traditional methods to the realities of cyberspace. This article explores a comprehensive approach to modernizing investigative operations, incorporating innovative technologies for big data collection and analysis, monitoring network activity, and identifying criminal schemes using artificial intelligence algorithms. Special attention is given to the need for developing computational infrastructure, analytical platforms, and cybersecurity systems to protect sensitive information from unauthorized access. The author emphasizes the importance of continuous professional development for operational personnel, including training in cyber intelligence methods, network protocol analysis, and cryptography, which are critical factors for effectiveness in the face of rapidly evolving threats. Simultaneously, the article examines the legal and ethical challenges associated with the digitalization of investigative activities. It discusses the necessity of balancing operational efficiency with the protection of citizens' rights, including personal data privacy and communication confidentiality. The study highlights the importance of establishing clear legal mechanisms and international standards for regulating digital evidence collection, cross-border information exchange, and preventing abuses. Risks such as algorithmic errors, false positives in data analysis systems, and ethical dilemmas of mass surveillance are analyzed. The role of transparency in law enforcement and collaboration with civil society in maintaining public trust is underscored. In conclusion, the article argues that successful digital transformation of investigative activities is only possible through the integration of technological innovations with traditional operational methods, enhanced interagency and international cooperation, and the creation of robust legal safeguards. A key condition is maintaining the principle of "human-centered decision-making" to minimize risks associated with automated systems and ensure compliance with democratic values.

For citation

Demchenko V.V. (2025) Teoreticheskiye i prakticheskiye aspekty sovershenstvovaniya operativno-rozysknoy deyatelnosti v usloviyakh tsifrovoy transformatsii sovremennogo obshchestva [Theoretical and Practical Aspects of Improving Investigative Activities in the Context of Digital Transformation of Modern Society]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (4A), pp. 345-356.

Keywords

Digital transformation, investigative activities, cybersecurity, big data, legal regulation.

References

1. Semenchuk V.V., Batoev V.B. Prerequisites for the formation of a concept for the development of operational investigative activities in the digital sphere (part 1) // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2023. No. 3 (66). pp. 132-136.
2. Tkachuk T.A., Kurysev K.N. Questions about decipherization in the aspect of operational investigative activities // Bulletin of the Vladimir Law Institute. 2023. No. 1 (66). pp. 107-111.
3. Ageenkov A.A., Efanov S.I. On certain problems of operational investigative activities in modern conditions // Bulletin of the Ryazan Branch of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 14. pp. 30-37.
4. Torop S.S. Digital capabilities in operational investigative activities // Bulletin of Young Scientists of Samara State University of Economics. 2023. No. 1 (47). pp. 122-126.
5. Timofeev S.V. Modern dominants in operational investigative activities // Philosophy of Law. 2024. No. 2 (109). pp. 180-186.
6. Ivanov P.I. Operational investigative activity in the conditions of digital reality: its scientific support // Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2022. No. 2 (68). pp. 64-67.
7. Turkaeva L.V. The legal essence of operational investigative activities of law enforcement agencies and its importance in the fight against crime // Law and order: history, theory, practice. 2020. No. 4 (27). pp. 66-70.
8. Yerkalov A.A. Law enforcement and acts of law enforcement in operational investigative activities // Legal Science. 2022. No. 6. pp. 91-96.
9. Iskaliev R.G. Improving the methods of operational investigative activities in modern conditions of digital transformation // Law and Law. 2023. No. 12. pp. 201-207.
10. Semenchuk V.V., Batoev V.B. Prerequisites for the formation of a concept for the development of operational investigative activities in the digital sphere (part 2) // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2023. No. 4 (67). pp. 165-174.
11. Shchetnev L.E. Legal and theoretical approaches to the essence of the operational investigative measure "Operational implementation" // Bulletin of the Vladimir Law Institute. 2023. No. 1 (66). pp. 112-115.
12. Babushkin V.A. Legislative bases of carrying out actions by internal affairs bodies in the field of operational and investigative analytics // A Russian investigator. 2020. No. 12. pp. 60-64.
13. Yakovets E.N. Some actual problems of theory and practice of operational investigative activity // Epom. 2020. No. 40. pp. 293-313.
14. Bely A.G., Surtsev A.V. Modern concepts of the system and principles of operational investigative activities // The Eurasian Law Journal. 2020. No. 8 (147). pp. 264-265.
15. Ivanov P.I. Operational investigative support of crime investigation: concept, essence and content // Bulletin of the Vladimir Law Institute. 2024. No. 2 (71). pp. 32-35.