

РЯСОВ Александр Алексеевич,
Профессор кафедры уголовного процесса и криминалистики
Ставропольского филиала Краснодарского университета МВД России,
кандидат юридических наук, доцент,
e-mail: mail@law-books.ru

БАГИРОВ Заур Русланович,
Старший преподаватель кафедры огневой подготовки
Северо-Кавказского института повышения квалификации
(филиал) Краснодарского университета МВД России,
e-mail: mail@law-books.ru

ПРОБЛЕМЫ ПОДГОТОВКИ ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА В ОБЛАСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Статья посвящена комплексному анализу актуальных проблем, связанных с подготовкой профессорско-преподавательского состава в области раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. В условиях стремительного роста киберпреступности и возрастающей сложности цифровых правонарушений, подготовка высококвалифицированных специалистов приобретает стратегическое значение для обеспечения национальной безопасности и общественного порядка.

Современные образовательные системы и правоохранительные структуры сталкиваются с серьёзными трудностями при формировании профессиональных компетенций у преподавательского состава. Основными барьерами, тормозящими процесс трансформации, являются несоответствие темпов цифровой трансформации и обновления учебных курсов, низкий уровень цифровой грамотности педагогов, дефицит актуального оборудования и слабо налаженная система непрерывного профессионального развития. Эти факторы снижают эффективность подготовки специалистов, способных оперативно реагировать на вызовы современности.

Для преодоления данных препятствий в статье предлагаются комплексные меры: создание целевых программ переподготовки, ориентированных на практическое освоение цифровых инструментов и методик; внедрение симуляционных, кейс-методов и геймифицированных форматов обучения, способствующих формированию реальных профессиональных навыков. Особое значение придаётся формированию устойчивых межведомственных связей между вузами и профильными органами — таким образом обеспечивается непрерывная адаптация образовательных стандартов к реальным потребностям рынка труда и оперативным задачам правоохранительной деятельности.

Ключевые слова: профессорско-преподавательский состав, подготовка кадров, киберпреступность, информационно-телекоммуникационные технологии, информационная безопасность, компьютерная криминалистика, практикоориентированный подход.

RYASOV Alexander Alekseevich,
Professor of the Department of Criminal
Procedure and Criminalistics of the Stavropol Branch
of the Krasnodar University of the Ministry of Internal Affairs of Russia,
Candidate of Law, Associate Professor

BAGIROV Zaur Ruslanovich,
Senior lecturer at the Department of Fire Training
of the North Caucasus Institute for Advanced Studies (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia

PROBLEMS OF TEACHING STAFF TRAINING IN THE FIELD OF DISCLOSURE AND INVESTIGATION OF CRIMES RELATED TO THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Annotation. The article is devoted to a comprehensive analysis of current problems related to the training of teaching staff in the field of disclosure and investigation of crimes committed using information and telecommunication technologies. In the context of the rapid growth of cybercrime and the increasing complexity of digital offenses, the training of highly qualified specialists is of strategic importance for ensuring national security and public order.

Modern educational systems and law enforcement agencies face serious difficulties in developing professional competencies among teaching staff. The main barriers hindering the transformation process are the discrepancy between the pace of digital transformation and the updating of training courses, the low level of digital literacy of teachers, the shortage of up-to-date equipment and a poorly established system of continuous professional development. These factors reduce the effectiveness of training specialists who are able to respond promptly to modern challenges.

To overcome these obstacles, the article suggests comprehensive measures: the creation of targeted retraining programs focused on the practical development of digital tools and techniques; the introduction of simulation, case-based methods and gamified learning formats that contribute to the formation of real professional skills. Special importance is attached to the formation of stable interdepartmental relations between universities and relevant authorities, thus ensuring the continuous adaptation of educational standards to the real needs of the labor market and the operational tasks of law enforcement.

Key words: faculty, staff training, cybercrime, information and telecommunication technologies, information security, computer forensics, practice-oriented approach.

Современный мир стремительно развивается благодаря информационным технологиям, и вместе с этим растет количество преступлений, совершаемых с использованием цифровых инструментов. Борьба с такими правонарушениями требует глубоких знаний и специфических навыков, которыми должны обладать сотрудники правоохранительных органов. Именно поэтому регулярное повышение квалификации сотрудников полиции становится неотъемлемой частью профессиональной деятельности.

Устойчивая диспропорция между учебными программами и реальными требованиями правоохранительной практики порождает цепную реакцию негативных последствий, угрожающих эффективности подготовки кадров в сфере расследования киберпреступлений.

Таким образом, курсанты и слушатели получают фрагментарные, устаревшие или поверхностные знания, не позволяющие им оперативно интегрироваться в рабочие процессы. Отсутствие системного подхода к формированию практических навыков превращает обучение в академическую формальность, а не в подготовку к реальным вызовам.

Кризис в подготовке кадров для цифровой криминалистики в системе МВД не сводится к количественному дефициту выпускников — он представляет собой фундаментальный системный дисбаланс, в котором опытные специалисты,

обладающие уникальными практическими компетенциями в области извлечения данных из зашифрованных носителей, восстановления следов в облачных экосистемах и реконструкции криптовалютных транзакций, оказываются заложниками оперативной необходимости. Их уход из практики не просто оставляет вакуум — он приводит к деградации институционального знания, поскольку передача опыта становится невозможной в условиях отсутствия формализованных механизмов наставничества и академической легитимации практики. В результате ключевые эксперты изолируются в рамках оперативных подразделений, их знания стагнируют, а новейшие угрозы остаются вне поля их внимания. Такая изоляция порождает парадокс: те, кто способен расследовать подобные преступления, становятся невидимыми для образовательной системы, а система, в свою очередь, теряет контакт с реальностью.

Преподавательский состав, в свою очередь, всё чаще состоит из специалистов, чьи профессиональные компетенции не обновлялись в течение нескольких лет. Их учебные материалы, зачастую основанные на устаревших методиках 2010-х годов, продолжают транслировать представления о цифровом следе как о физическом артефакте, хранящемся на жёстких дисках, и о расследовании как о последовательности шаблонных действий, применимых к устаревшим

ОС. В то же время современные преступные практики смещаются в сторону асинхронных, динамичных и децентрализованных сред: Telegram-каналы с эфемерными сообщениями, блокчейн-транзакции, скрытые в смарт-контрактах, и AI-генерируемые подделки, не оставляющие традиционных цифровых отпечатков. Выпускники, прошедшие такое обучение, оказываются не подготовленными к интерпретации следов, не существующих в рамках их учебных моделей — они не умеют деконструировать структуру анонимных сетей, не знакомы с инструментами автоматизированного сбора данных из социальных платформ. Таким образом, образовательная система производит не специалистов, а «пользователей прошлого» — людей, воспринимающих цифровой мир как черно-белый архив, в то время как преступность уже давно перешла в многомерное, адаптивное и самообучающееся пространство.

Не менее критичен разрыв между учебными программами и инструментальной базой оперативной практики. Обучаемые осваивают симуляторы, созданные десятилетия назад, с интерфейсами, которые давно вышли из эксплуатации, и алгоритмами, заменёнными на более мощные, адаптивные и облачно-ориентированные решения. В реальных следственных подразделениях используются специализированные платформы для анализа сетевой активности, распознавания лиц в реальном времени, восстановления зашифрованных архивов и трассировки криптовалютных потоков — инструменты, о которых курсанты и слушатели узнают лишь на третьем курсе, если вообще узнают. В результате при поступлении на службу выпускники сталкиваются не с применением знаний, а с полной перезагрузкой компетенций: они вынуждены учиться у коллег, отнимая у них рабочее время, теряя до 6–8 месяцев на адаптацию и снижая общую оперативную эффективность подразделений. Причина не в низкой мотивации или недостаточной подготовке обучающихся — она коренится в институциональной консервативности, бюрократических барьерах, страхе перед изменением протоколов доступа и неспособности организовать безопасное, контролируемое внедрение реальных инструментов в учебный процесс.

При этом технологическая доступность решений позволяет предложить альтернативу. Даже в условиях строгой секретности и ограничений на доступ к федеральным базам данных можно создать демонстрационные версии служебных компьютерных программ — с анонимизированными сценариями, симулированными данными, ограниченными функциональными модулями и жёсткими протоколами безопасности. Такие среды не заменяют реальные рабочие

инструменты, но позволяют будущим специалистам освоить логику интерфейсов, понять архитектуру запросов, научиться интерпретировать результаты анализа и осознавать взаимодействие между модулями. Это не роскошь, а стратегическая необходимость — условие для преодоления когнитивного диссонанса между теорией и практикой. Реализация такого подхода требует не просто технических решений, а перестройки системы межведомственного взаимодействия: между вузами и оперативными подразделениями, между педагогами и разработчиками программного обеспечения, между руководством и техническими службами. Необходима не просто координация, а формирование инновационного экосистемного контракта, в рамках которого образование становится не пассивной трансляцией знаний, а активной, адаптивной и динамично обновляемой практикой. Без этого мы не готовим следователей будущего — мы воспроизводим устаревшие роли, обречённые на неэффективность в мире, который уже ушёл далеко вперёд.

Современные оперативно-розыскные и следственные подразделения МВД активно используют специализированные программные комплексы (например, «Розыск», «Сова», «Поток», «Папилон» и др.). Однако вузы МВД не имеют доступа к этим системам, из-за чего:

- Следователь не может быстро проверить данные по криптовалютам, потому что в вузе не работал с анализаторами блокчейна.
- Оперативник не умеет эффективно искать связи между фигурантами, так как не использовал систему «Поток».
- Криминалист не знает, как правильно извлекать цифровые улики с помощью современных криминалистических комплексов.

Причин, по которым складывается такая ситуация несколько:

1. Прежде всего это ограниченный бюджет. Вопрос финансирования образовательных учреждений системы МВД действительно вызывает серьёзные опасения относительно качества подготовки специалистов, призванных обеспечивать безопасность граждан и стабильность государства. Финансовая недостаточность препятствует приобретению необходимого оборудования, современных лицензионных программных продуктов и заключению контрактов с внешними экспертами и специализированными компаниями, предоставляющими услуги дополнительного профессионального образования и консультационной поддержки.

Министерство внутренних дел в этом вопросе традиционно стремится минимизиро-

вать расходы на взаимодействие с другими ведомствами, предпочитая полагаться исключительно на собственные ресурсы и возможности. Такая политика имеет очевидные недостатки, проявляющиеся в ограниченных возможностях для внедрения новых методов и технологий обучения, недостаточной осведомлённости преподавателей о последних достижениях в области борьбы с киберпреступностью и иными сложными видами противоправных деяний.

Преодолеть обозначенные трудности возможно лишь посредством комплексной организации взаимодействия различных субъектов правоохранительной системы. Здесь ключевое значение приобретает взаимодействие подразделений Министерства внутренних дел, занятых созданием и поддержкой специализированного программного обеспечения, с образовательными учреждениями высшего профессионального образования. Необходимо обеспечить тесное сотрудничество между этими структурами для разработки адаптированных версий программных комплексов, предназначенных исключительно для учебно-методических целей.

Создание специальных версий должно учитывать необходимость сохранения ключевых функциональных характеристик оригинального программного продукта, обеспечивая при этом строгий контроль доступа к конфиденциальной информации. Такая задача предъявляет повышенные требования к квалификации специалистов-разработчиков, уровню технической компетентности и качеству правовой поддержки проектов подобного уровня.

Важно отметить, что такая инициатива нуждается не только в инициативе руководителей вузов, но и в принятии нормативных актов на уровне самого министерства. Так, потребуются заключение специальных соглашений о сотрудничестве, внесение поправок в ведомственные приказы и регламенты, регулирующие порядок эксплуатации программного обеспечения. Эти процедуры позволят легализовать применение демонстрационного программного обеспечения в учебном процессе и создать правовые основания для дальнейшей работы с ним.

Подобная мера позволила бы существенно повысить качество подготовки специалистов, приблизив условия обучения к реальным условиям работы сотрудников органов внутренних дел. Курсанты и слушатели смогли бы освоить специфику использования специализированных программных комплексов, познакомиться с алгоритмами принятия решений и отработать навыки анализа и обработки информации в режиме реального времени.

2. Наконец, не маловажной причиной является инертность образовательной системы МВД

России. К сожалению, далеко не все ответственные за обучение лица вникают и в достаточной степени разбираются во всех вышеуказанных проблемах, что выражается в слабой восприимчивости к выявленным трудностям и неспособности изменить устоявшиеся схемы действий, результатом чего становится уклонение ряда должностных лиц от активного участия в реформах, сопровождающееся созданием иллюзии активной деятельности путём оформления множества второстепенных бумаг, совещаний, планов, отчетов, дорожных карт, координационных советов, бесконечных совещаний и т.д., что формирует своеобразную псевдокультуру занятости, направленную на сохранение существующего порядка вещей, не требующих каких-либо изменений и поддержание поверхностного восприятия успехов.

Следствием подобного поведения становится существенное отвлечение преподавательского состава от основной миссии — самообразования и освоения новых методик преподавания, поскольку значительная доля рабочего времени расходуется на формальное документирование незначительных аспектов, устранение мелких недостатков или получение одобрения стандартных процедур. Кроме того, в настоящее время в системе МВД России вообще отсутствуют программы переподготовки преподавателей по линии расследования киберпреступлений.

В целях преодоления сложившейся ситуации, на наш взгляд, необходимы комплексные меры, направленные на улучшение подготовки преподавательского состава к которым можно отнести:

- организацию регулярных курсов повышения квалификации специально ориентированных на изучение новейших методов цифровой криминалистики и анализа данных. Особенно важным является проведение таких занятий не в ВУЗах МВД России, а в сторонних организациях, специализирующихся на выявлении и предотвращении инцидентов в сфере цифровой безопасности. Такими организациями могут являться Национальный координационный центр по компьютерным инцидентам (НКЦКИ), Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России), «Лаборатория Касперского», компания «Элкомсофт» и др.

Безусловно, можно согласиться с мнением Н.Р. Шевко [1, с.89] о том, что это требует значительных средств, однако иначе проблемы не исправить. Не плохим опытом, в данном направлении, является созданный в Московском университете МВД России имени В.Я. Кикотя, при взаимодействии со Сбербанком и ВТБ, отделения банков на полигонной базе, что обеспечивает возможность проведения практических занятий по типичным в данной сфере фабулам [2, с.268]. Однако это сделано в большей степени для обучающихся, а не для преподавательского состава и может быть использовано разово, исключительно в рамках рассмотрения отдельных тем.

- привлечение ведущих практикующих экспертов, как МВД России, проводящих компьютерные экспертизы, так и экспертов других министерств и ведомств. В целях повышения эффективности подготовки профессорско-преподавательского состава представляется необходимым приглашение для проведения занятий с ними сотрудников следственных и оперативно-розыскных подразделений, специализирующихся на раскрытии и расследовании вышеуказанных преступлений. Сотрудничество с действующими сотрудниками подразделений кибербезопасности позволит обогатить учебный процесс реальными примерами и ситуациями и ознакомить их с новыми способами как совершения, так и расследования киберпреступлений.
- привлечение к разработке специализированных учебных программ вышеуказанных специалистов, что позволит избежать ситуаций, когда учебные заведения МВД работают с устаревшими или упрощёнными программами, что серьёзно влияет на подготовку будущих сотрудников.

Актуальность вопроса несостыковки учебных программ высших учебных заведений МВД с практическими требованиями оперативной службы обусловлена отсутствием полноценной взаимосвязи теории и практики. Несоответствие образовательной составляющей реальным требованиям оперативно-служебной деятельности порождает ряд серьёзных проблем, препятствующих формированию у выпускников необходимых профессиональных качеств и компетенций.

Одним из приоритетных направлений устранения указанного разрыва является качественная подготовка профессорско-преподава-

тельского состава и внедрение эффективных механизмов взаимодействия университетов с подразделениями ведомства. Предоставление учебным заведениям специального доступа к тестовым версиям используемых программных средств и информационным массивам позволит будущим сотрудникам ознакомиться с актуальным инструментарием и технологической средой, применяемой органами правопорядка.

Формирование высокопрофессиональных кадров в сфере правоохранительной деятельности требует консолидации усилий государственного аппарата, образовательных организаций и научного сообщества. Лишь скоординированные усилия всех заинтересованных сторон способны устранить имеющиеся диспропорции и подготовить высококвалифицированные кадры, способные эффективно решать задачи борьбы с современными проявлениями преступности.

Список литературы:

[1] Шевко, Н.Р. Проблемы подготовки специалистов по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России / Н. Р. Шевко // Вестник Казанского юридического института МВД России. – 2017. – № 1(27). – С. 87-89.

[2] Иванов, Д.А. Подготовка специалистов для органов предварительного расследования в условиях противодействия преступлениям, совершаемых с использованием информационно-телекоммуникационных технологий / Д.А. Иванов, В.В. Артемова, С.В. Ермаков // Вестник экономической безопасности. – 2022. – № 2. – С. 265-270.

References:

[1] Shevko, N.R. Problems of training specialists in solving and investigating crimes committed using modern information technologies in educational organizations of the Ministry of Internal Affairs of Russia/N.R. Shevko//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. – 2017. – № 1(27). – S. 87-89.

[2] Ivanov, D.A. Training of specialists for preliminary investigation bodies in the context of countering crimes committed using information and telecommunication technologies/D.A. Ivanov, V.V. Artemova, S.V. Ermakov//Bulletin of Economic Security. – 2022. – № 2. – S. 265-270.

