



Профессиональный ответ на вызовы киберпреступности: формирование кадрового потенциала для современного уголовного судопроизводства

Н. А. Моругина

Кандидат юридических наук, доцент,
доцент кафедры уголовного процесса

Воронежский институт МВД России
394065, Россия, г. Воронеж, пр-т Патриотов, 53

E-mail: moruginy@mail.ru

Аннотация: в статье исследованы вопросы цифровой трансформации уголовного судопроизводства в условиях динамичного развития высоких технологий и необходимости повышения эффективности правоприменительной практики. Особое внимание уделяется анализу структуры и содержания профессиональных компетенций участников уголовного судопроизводства в контексте современных требований и инновационных подходов. Обосновывается необходимость системных изменений образовательной и кадровой политики, которые направлены на реализацию положений национального проекта «Цифровая экономика Российской Федерации» в части решения проблемы обеспечения квалифицированными кадрами для борьбы с киберпреступностью. Основным звеном такой модернизации в структуре юридических вузов автор видит специализированные подразделения – своеобразные «цифровые кафедры», задачей которых станет подготовка специалистов, способных эффективно применять цифровые технологии в сфере уголовного судопроизводства и правоприменительной деятельности.

© Моругина Н. А., 2026



Эта работа распространяется по лицензии CC BY 4.0.
Чтобы просмотреть копию этой лицензии, посетите
<https://creativecommons.org/licenses/by/4.0/>

Ключевые слова: цифровая трансформация, цифровые компетенции, цифровая кафедра, специалист в сфере расследования компьютерных преступлений, IT-следователь

Professional Response to Cybercrime Challenges: Building Human Resources for Modern Criminal Proceedings

N. A. Morugina

Voronezh Institute of the Ministry of Internal Affairs of Russia
53, Patriotov prospect, Voronezh, 394065, Russia

E-mail: moruginy@mail.ru

Abstract: *the article explores the issues of digital transformation of criminal proceedings in the context of the dynamic development of high technologies and the need to improve the efficiency of law enforcement practice. Special attention is paid to analyzing the structure and content of the professional competencies of participants in criminal proceedings in the context of modern requirements and innovative approaches. The article substantiates the need for systemic changes in educational and personnel policies aimed at implementing the provisions of the national project "Digital Economy of the Russian Federation" in terms of addressing the issue of providing qualified personnel to combat cybercrime. As the main link in this modernization, the author sees specialized units in the structure of law schools, such as "digital departments", whose task will be to train specialists who can effectively use digital technologies in criminal proceedings and law enforcement.*

Keywords: *digital transformation, digital competencies, digital department, computer crime investigator, IT investigator*

Цифровая трансформация уголовного судопроизводства, обусловленная объективным развитием технологий и необходимостью повышения эффективности правоприменительной деятельности, выходит далеко за рамки внедрения в уголовное судопроизводство цифровых платформ и электронных сервисов. В условиях, когда традиционные методы сбора и оценки доказательств уступают место современным цифровым подходам, необходима адаптация образовательных программ и методов обучения для формирования у будущих правоприменителей соответствующего набора цифровых компетенций.

С учетом обозначенной потребности особую актуальность приобретает вопрос о структуре и содержании профессиональных компетенций. В этой ситуации интересна позиция Т. Ю. Марковой и Т. Ю. Максимовой, согласно которой подготовка кадров для органов предварительного расследования в цифровой среде должна

быть ориентирована на то, чтобы сформировать три группы профессиональных компетенций:

1) *коммуникативные компетенции в цифровой среде*, включающие владение технологиями дистанционного взаимодействия, к примеру видео-конференц-связью, специализированными платформами, в перспективе – технологиями голографических звонков, а также применение веб-форм для интервьюирования и чат-ботов для первичного консультирования участников уголовного судопроизводства;

2) *аналитические компетенции на основе цифровых технологий*, то есть умение использовать автоматизированные информационно-поисковые и аналитические системы (включая инструменты на базе искусственного интеллекта) для анализа обстоятельств дела, поиска правовых решений и судебной практики, а также возможности IT-криминалистики и программ 3D-визуализации событий преступления;

3) *технологические компетенции* – владение технологией голосового ввода, использование шаблонов из справочных правовых систем и облачных сервисов для хранения документов¹.

В научной публикации отечественных ученых Д. И. Чуковой, Д. А. Медведева и М. В. Литвиненко представлена модель формирования компетенций специалиста в сфере расследования компьютерных преступлений, в рамках которой авторами предложены три ключевые профессиональные компетенции, а именно:

1) *компетенция в области организации и планирования расследования киберпреступлений, совершенных с использованием средств вычислительной техники*, то есть способность специалиста осуществлять комплекс организационно-плановых мероприятий, которые направлены на выявление, документирование и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий (ИКТ);

2) *компетенция в области применения программно-аппаратных и инструментальных средств для проверки работоспособности и оценки эффективности систем защиты информации*, то есть способность специалиста использовать современные вычислительные и программные средства, языки и системы программирования для решения профессиональных задач в области киберрасследований;

3) *компетенция по обработке и использованию юридически значимой информации*, то есть способность специалиста осуществлять сбор, накопление, обработку и анализ информации, имеющей значение для раскрытия и расследования киберпреступлений².

Практическая востребованность такой детализации цифровых компетенций находит прямое подтверждение в эволюции развития правоприменительных структур

¹ Маркова Т. Ю., Максимова Т. Ю. Трансформация профессиональных навыков в условиях цифровизации уголовного судопроизводства // Право и политика. 2023. № 6. С. 27–34.

² Чукова Д. И., Медведев Д. А., Литвиненко М. В. Модель формирования компетенций специалиста в сфере расследования компьютерных преступлений // Вопросы кибербезопасности. 2019. № 3 (31). С. 59–60.

в области борьбы с киберпреступностью³. Ключевым шагом в данном направлении стала реорганизация 2022 года, когда в соответствии с Указом Президента России В. В. Путина⁴ в структуре МВД России было создано новое подразделение – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК МВД России)⁵, пришедшее на смену Управлению «К» МВД России (просуществовало с 13 августа 1998 года по 1 февраля 2023-го), с довольно объемным набором ключевых задач, таких как:

- выявление, предупреждение, пресечение и раскрытие преступлений и иных правонарушений в сфере ИКТ;
- обеспечение координации подразделений МВД России, участвующих в расследовании преступлений, совершаемых с использованием ИКТ;
- анализ данных из информационно-телекоммуникационных сетей для выявления противоправной активности;
- взаимодействие с государственными органами, организациями ИКТ-сектора, финансовыми институтами и субъектами РФ в области обеспечения информационной безопасности;
- разработка предложений по совершенствованию законодательства в сфере кибербезопасности и противодействия киберпреступности;
- организация профилактической работы, направленной на снижение числа преступлений, совершаемых с использованием сети Интернет.

В состав подразделения УБК МВД России, согласно официальным данным, входят профильные специалисты министерства, имеющие необходимые знания и опыт для эффективной работы по данному направлению⁶. Одновременно статистические данные МВД России за январь – июль 2025 года демонстрируют разноплановую динамику ключевых показателей ИТ-преступности. Несмотря на заметное (на 2,3 %) снижение общего количества преступлений данной категории (424,9 тыс.), фиксируется существенный (на 16 %) рост материального ущерба – со 100,5 до 119,6 млрд рублей⁷. Приведенное расхождение в статистике свидетельствует о том, что организационно-

³ «Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных» (Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45).

⁴ О внесении изменений в некоторые акты Президента Российской Федерации: указ Президента Рос. Федерации от 30 сент. 2022 г. № 688.

⁵ Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России: приказ МВД России от 29 дек. 2022 г. № 1110.

⁶ История УБК МВД России. URL.: <https://34.mvd.rf/gu-mvd/структура/подразделения-gu/отдел-по-борьбе-с-противоправным-использ/история>.

⁷ В России за январь – июль 2025 г. ущерб от ИТ-преступлений вырос на 16 % и составил почти 120 млрд руб. URL.: <https://alrf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd/>.

кадровых мер, выразившихся в создании УБК МВД России, недостаточно для кардинального изменения ситуации. В этой связи полагаем, что существенное внимание необходимо уделять профессиональной переподготовке кадров.

Сделанный вывод находит свое эмпирическое подтверждение в исследованиях, проведенных П. М. Олейником, И. В. Ильиным и С. Н. Суховым, которые, в рамках педагогической деятельности исследовав профессиональные компетенции слушателей факультета переподготовки и повышения квалификации Нижегородской академии МВД России и слушателей Нижегородского филиала Санкт-Петербургской академии Следственного комитета России, выявили системную проблему в их профессиональной подготовке. В частности, был зафиксирован дефицит знаний в области обращения с компьютерной техникой и специализированным программным обеспечением. Отдельно отмечен недостаточный уровень компетенции следователей ОВД в вопросах, связанных с назначением судебной компьютерно-технической экспертизы⁸. Не менее убедительное обоснование данная проблема находит в результатах анкетирования 134 дознавателей и следователей, проведенного Ф. К. Зиннуровым и Э. Т. Хайрулловой. В частности, полученные учеными результаты продемонстрировали, что для абсолютного большинства респондентов (78 %) цифровая информация остается вне поля их профессионального внимания, при этом оставшиеся 22 % опрошенных ориентируются на знания специалистов⁹. Считаем, что в этой связи у сотрудников органов предварительного расследования формируется дефицит цифровой грамотности, который обладает признаком системности, поскольку обусловлен не только индивидуальными пробелами в подготовке отдельных специалистов, но и комплексом объективных факторов: стремительной эволюцией ИКТ, латентностью и трансграничным характером киберпреступлений, а также относительно медленными темпами адаптации образовательных и ведомственных стандартов к новым цифровым реалиям.

На сегодняшний день специалист по расследованию компьютерных преступлений, по мнению уже упомянутых авторов, должен обладать знаниями на стыке трех областей профессиональной деятельности: юриспруденции, информатики и вычислительной техники и информационной безопасности¹⁰. Данная трехкомпонентная модель, представляющая собой сумму знаний из трех дисциплин, безусловно, задает важные системные координаты для подготовки кадров, однако не отражает динамического внедрения этих знаний в модели «навык + компетенция».

С учетом этого принципиальное значение приобретает подход, предложенный учеными С. В. Зуевым и А. И. Зазулиным, который фокусируется именно на формировании практико-ориентированного образа IT-следователя для борьбы с киберпре-

⁸ Олейник П. М., Ильин И. В., Сухов С. Н. Актуальные проблемы образовательного процесса и использования аппаратно-программных комплексов и программного обеспечения в деятельности правоохранительных органов // Вестник Нижегородского университета им. Н. И. Лобачевского. 2019. № 6. С. 157–160.

⁹ Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. Т. 9, № 2 (32). С. 276.

¹⁰ См.: Чукова Д. И., Медведев Д. А., Литвиненко М. В. Указ. соч. С. 58.

ступностью. Согласно изложенной учеными концепции, ядро профессиональной компетентности IT-следователя образует следующий комплекс взаимосвязанных навыков: работа с большими данными (умение анализировать, структурировать и интерпретировать большие объемы цифровой информации); понимание компьютерно-технических экспертиз (способность читать и анализировать заключения экспертов любой сложности); владение цифровыми технологиями расследования (знание методов обнаружения, фиксации и изъятия цифровых следов); широкое применение электронных документов и в перспективе использование электронного помощника. Авторы подчеркивают, что предложенный набор компетенций не может быть обеспечен в рамках традиционных образовательных траекторий; по их мнению, подготовка IT-следователей должна осуществляться по специальным образовательным программам, сочетающим в себе как теоретические курсы, подготовленные ведущими учеными в сфере цифровизации уголовного процесса, так и практические занятия с экспертами-программистами, объясняющими, как работают и как могут применяться те или иные цифровые технологии. Коллеги справедливо отмечают, что «создание таких программ обучения и подготовки кадров, основанных на триединстве теории, практики и экспертизы, является важной предпосылкой не только введения института IT-следователей, но и его последующего эффективного функционирования»¹¹.

В этой связи обоснованной и актуальной выглядит позиция профессора О. А. Малышевой, которая справедливо указывает на то, что для качественного и своевременного раскрытия и расследования преступлений, совершаемых в цифровой среде, сотрудникам правоохранительных органов необходимы специальные знания и умения, выходящие за рамки классического юридического образования. Предложенный автором перечень компетенций¹² для сотрудников правоохранительных органов при расследовании киберпреступлений, состоящий из одиннадцати компонентов, может быть структурирован в несколько ключевых профессиональных блоков:

1) *криминалистико-технический блок (оперативное обеспечение)*, формирующий основу для самостоятельного проведения первоначальных следственных и процессуальных действий, к которому относятся: уверенная работа с цифровой информацией независимо от форматов ее существования (п. 1); правильное изъятие и упаковка носителей электронной информации, исключающие возможность ее искажения или утраты, а также обеспечение сохранности данных на протяжении всего периода досудебного производства (п. 4, 7); владение методикой выявления и фиксации электронных доказательств (п. 8), технологией автоматизированного рабочего места (п. 9) и эксплуатацией сетевого оборудования (п. 10);

2) *аналитико-оценочный блок (процессуальное мышление)*, обеспечивающий анализ цифрового следа и его интеграцию в общую доказательственную базу, который включает в себя: способность верно оценивать относимость к делу сведений, закрепленных на электронном носителе (п. 2); определять факты и средства фальси-

¹¹ Зуев С. В., Зазулин А. И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. 2024. № 2. С. 51.

¹² Малышева О. А. О новом векторе профессиональной подготовки следователя в условиях цифровой трансформации // Вестник Томского государственного университета. 2022. № 480. С. 267.

фикации (искажения) электронной информации (п. 11); преобразовывать (при необходимости) цифровую информацию в аналоговый формат без искажения с помощью специальных устройств и программных средств (п. 3);

3) *экспертно-организационный блок (управление расследованием)*, являющийся ключевым в постановке задач специалисту, охватывающий: определение вида судебной компьютерно-технической экспертизы (п. 5); создание и уверенную работу с виртуальным хранилищем следов IT-преступлений (п. 6).

Необходимость формирования соответствующего набора компетенций распространяется не только на сотрудников органов предварительного расследования, занимающихся киберпреступлениями, но и на специалиста, с участием которого в соответствии с частью 2 статьи 164.1 Уголовно-процессуального кодекса РФ¹³ изымаются электронные носители информации, «когда необходимы его специальные познания для обнаружения, закрепления и изъятия предметов и документов, применения техсредств, разъяснения вопросов, входящих в его профессиональную компетенцию»¹⁴. В этой связи аргументированной выглядит позиция профессора П. С. Пастухова, предлагающего включить в перечень профессиональных компетенций специалиста умения восстанавливать данные, осуществлять поиск документов, преобразовывать мультимедиа, а также реализовывать иные функции, отражающие комплексный характер его профессиональной деятельности, где ключевым условием является обеспечение сохранности изъятых данных в неизменном виде¹⁵. При этом ученый небезосновательно говорит об отсутствии в настоящее время в России стандартов для аккредитации, сертификации и образования специалистов цифровой судебной профессии, отмечая при этом, что наиболее системная и детализированная нормативная база, регулирующая процедуры обращения с цифровыми следами, сложилась в Великобритании.

Прежде всего, британский опыт характеризуется поэтапным формированием целого комплекса специализированных актов – правил, рекомендаций и руководств, закрепляющих процессуально выверенный порядок сбора и анализа цифровых доказательств. Исторически данный процесс можно проследить с 2007 года, когда было принято техническое руководство, регламентирующее хранение, воспроизведение и удаление цифровых изображений. В 2010 году разрабатывается и вводится в действие практическое руководство по собиранию компьютерных доказательств, а в 2014-м – практическое руководство, адаптированное к работе с цифровыми следами преступлений в целом. В 2016 году в руководстве по анализу сайтов, местоположения абонентов даются рекомендации по получению необходимой доказательственной информации из технических устройств и от соответствующих провайдеров связи, а также обработке этих данных. В 2017 году руководство по обеспечению достовер-

¹³ Уголовно-процессуальный кодекс Российской Федерации: Федер. закон от 18 дек. 2001 г. № 174-ФЗ: принят Гос. Думой 22 нояб. 2001 г.: одобрен Советом Федерации 5 дек. 2001 г. (ред. от 09.04.2026).

¹⁴ *Малыгин К. В.* Проблемы вовлечения электронных данных в уголовное судопроизводство // *Ex iure*. 2023. № 2. С. 155.

¹⁵ *Пастухов П. С.* О необходимости развития компьютерной криминалистики // *Пермский юридический альманах*. 2018. № 1. С. 454.

ности, пригодности и надежности цифровых доказательств закрепляет требования к ресурсам, техническим средствам, конкретным шагам, ограничениям и желаемым результатам¹⁶. Примечательно, что эти документы, представляющие собой свод конкретных методик и стандартизированных процедур, детально описывают допустимые способы работы с цифровой информацией сотрудников правоохранительных органов при расследовании киберпреступлений.

В этой связи стоит отметить, что в 2015 году в России был введен в действие ГОСТ Р ИСО/МЭК 27037-2014¹⁷ – национальный стандарт (далее – Стандарт), идентичный международному стандарту ISO/IEC 27037:2012¹⁸ и регламентирующий процедурные аспекты работы с доказательствами в цифровой форме. В Стандарте раскрываются процессы идентификации, сбора, изъятия и сохранения доказательств, а кроме того, детализируются категории привлекаемых специалистов и вводятся, наряду с традиционными экспертами, две принципиально новые фигуры:

1) специалист оперативного реагирования по свидетельствам, представленным в цифровой форме (Digital Evidence First Responder, DEFR), – физическое лицо, уполномоченное, обученное и подготовленное к первоначальным действиям на месте, ответственное за первичный сбор и изъятие цифровых свидетельств с обеспечением их сохранности;

2) специалист по свидетельствам, представленным в цифровой форме (Digital Evidence Specialist, DES), – физическое лицо, обладающее специальными знаниями, навыками, способностями, чтобы разбираться в широком спектре технических вопросов.

Таким образом, Стандарт регулирует не только общее руководство по работе с цифровыми следами, но и разделяет участников, выделяя оперативного специалиста (DEFR) для работы на месте происшествия (функционально эта фигура аналогична эксперту, входящему в состав следственно-оперативной группы) и технического специалиста (DES) для комплексного анализа цифровых следов (его полномочия сопоставимы с полномочиями эксперта-криминалиста, которому поручается проведение экспертиз).

Отметим, что в приложении к Стандарту содержится структурированная модель цифровых компетенций, необходимых специалисту, которая классифицирует требования по трем уровням профессиональной подготовки:

1) *осведомленность* – базовый уровень, подразумевающий способность специалиста к распознаванию, идентификации и пониманию информации, доступной в цифровых устройствах, базах данных, генерируемых системой записях; определению состояния устройства; оценке значения доказательной информации; следственному анализу Сети и связанных с ней устройств и т.д.;

¹⁶ Пастухов П. С. Указ. соч. С. 459.

¹⁷ 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. Введ. 2015–11–01. М.: Стандартиформ, 2014. URL: <https://docs.cntd.ru/document/1200112857>.

¹⁸ ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL.: <https://www.iso.org/standard/44381.html>.

2) *знания* – уровень компетентности, формируемый в результате профессионального обучения (к примеру, по программе повышения квалификации, профессиональной подготовки или переподготовки) либо накопленного опыта в практической деятельности в соответствующей сфере. Данный уровень характеризуется наличием систематизированных теоретических и прикладных знаний, достаточных для самостоятельного выполнения специалистом комплексных задач, таких как создание образа цифрового носителя информации в целом или его части, определение параметров документирования информации, описание процесса сбора цифровой информации, проведение опроса подозреваемых и т.д.;

3) *умения* – высший уровень компетентности, так как специалист данного уровня может самостоятельно, без внешнего контроля/надзора, реализовывать поставленные перед ним задачи и принимать соответствующие решения в рамках своей профессиональной деятельности (определение паролей, связывание IP-адресов и MAC-адресов для идентификации устройства в Сети и т.д.).

Считаем, что эффективность данной модели на практике напрямую зависит от ее внедрения в образовательные стандарты и программы высшего образования. В этой связи целесообразен критический анализ действующих правовых документов, регламентирующих подготовку специалистов в области юриспруденции. Так, детальное изучение приказа Минобрнауки от 13 августа 2020 г. № 1011 «Об утверждении федерального государственного образовательного стандарта высшего образования (ФГОС) – бакалавриат по направлению подготовки 40.03.01 Юриспруденция» позволило выделить ключевую проблему, которая может возникнуть при подготовке специалиста для противодействия киберпреступности, а именно *формальное наличие цифровых компетенций*.

В частности, пункт 3.3 ФГОС включает общепрофессиональную компетенцию ОПК-8 («способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности») и ОПК-9 («способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности»). Однако отметим, что *практическое воплощение данных компетенций в учебном плане сводится к изучению единственной дисциплины* – «Информационные технологии в юридической деятельности» (п. 2.2), что представляется явно недостаточным для формирования полноценных навыков у будущих специалистов по борьбе с киберпреступлениями и реализации паспорта национального проекта «Цифровая экономика Российской Федерации»¹⁹, предполагающей целенаправленную государственную политику в области развития кадрового потенциала IT-отрасли (D8).

Напомним, что данный нацпроект ориентирован на преодоление структурного дефицита специалистов высшей квалификации в информационно-технологической сфере. Основные механизмы достижения этой цели – разработка и внедрение новых

¹⁹ Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”»: утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. URL: <https://base.garant.ru/72296050/>.

образовательных программ, отвечающих запросам цифровой индустрии, привлечение к преподавательской деятельности практиков из IT-индустрии, непрерывное развитие кадрового потенциала самих образовательных организаций посредством реализации программ повышения квалификации и профессиональной переподготовки в области информационных технологий.

Представляется также, что для реализации ключевых механизмов национальной программы «Цифровая экономика Российской Федерации» в части кадрового обеспечения сферы противодействия киберпреступности необходима системная модернизация образовательной экосистемы. Одним из ключевых институциональных элементов такой модернизации должно стать целенаправленное формирование и развитие в вузах страны профильных структурных подразделений – специализированных «цифровых кафедр»²⁰.

Концепция создания «цифровой кафедры» должна быть ориентирована на учреждение научно-образовательных подразделений, аккумулирующих в единой форме компетенции на стыке юриспруденции, цифровой криминалистики, программирования, судебной экспертизы, информационных технологий и информационной безопасности. Целью деятельности таких подразделений станет преодоление междисциплинарного разрыва и обеспечение сквозной интеграции IT-знаний в традиционную правовую подготовку.

Прецеденты успешного функционирования «цифровых кафедр» в образовательной практике уже существуют и подтверждают жизнеспособность данного подхода. В качестве примера можно привести:

- кафедру информационных технологий и организации расследования киберпреступлений в Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева, ориентированную на подготовку специалистов для органов предварительного следствия в цифровой среде;

- кафедру компьютерной безопасности и технической экспертизы в Воронежском институте МВД России, подготавливающую специалистов по информационно-аналитической экспертизе компьютерной информации, а также по организации противодействия преступлениям, совершаемым с использованием IT-технологий;

- кафедру противодействия преступлениям в сфере информационно-телекоммуникационных технологий в Московском университете МВД России им. В. Я. Кикотя, осуществляющую подготовку специалистов по выявлению, раскрытию, расследованию и предупреждению различных видов преступлений, совершаемых в информационно-телекоммуникационной сфере.

Полагаем, что создание подобных кафедр в ведущих вузах страны позволит решить ряд стратегических задач, а именно: сконцентрировать интеллектуальные и материально-технические ресурсы для разработки и реализации инновационных образовательных программ по соответствующим направлениям; сформировать постоянный штат квалифицированного профессорско-преподавательского состава, сочетающего фундаментальную юридическую подготовку с глубокими знаниями и прак-

²⁰ Именно с таким названием создана и функционирует кафедра в Южно-Уральском государственном университете (национальном исследовательском университете).

тическими навыками в области IT-технологий; создать базовые площадки для проведения прикладных научных исследований; обеспечить преемственность и развитие компетенций через построение вертикали знаний будущих специалистов в рамках единой научно-педагогической школы.

Кроме того, для подготовки конкурентоспособных специалистов в области борьбы с киберпреступностью важно разработать и внедрить в учебный процесс образовательные программы междисциплинарного характера, построенные на стыке ключевых областей знаний: права, цифровой криминалистики, судебной экспертизы, информационных технологий, программирования и информационной безопасности.

Структурно-содержательным элементом в планах рабочих программ должен выступать практико-ориентированный подход к подготовке специалистов в области борьбы с киберпреступностью, включающий в себя следующие инновационные методики преподавания: имитационный метод – проведение деловых игр (имитация осмотра места происшествия с применением цифровых технологий фиксации и работы с цифровыми следами, проведение следственных действий с помощью видеоконференц-связи и т.д.); технологическое моделирование – применение 3D-сканеров и средств виртуальной реальности (VR) для реконструкции следственных действий (осмотр места происшествия, следственный эксперимент) в среде, максимально приближенной к реальности, с интеграцией технологий искусственного интеллекта в образовательную деятельность; систематическое привлечение к преподавательской деятельности практикующих IT-специалистов и экспертов-криминалистов.

Библиографический список

Зиннуров Ф. К., Хайруллова Э. Т. Особенности работы с электронными носителями как источниками доказательств при проведении следственных действий // Вестник Казанского юридического института МВД России. 2018. Т. 9, № 2 (32). С. 274–278. DOI: 10.24420/KUI.2018.32.13978.

Зув С. В., Зазулин А. И. IT-следователь в цифровой среде уголовного судопроизводства // Правопорядок: история, теория, практика. 2024. № 2. С. 48–54. DOI: 10.47475/2311-696X-2024-41-2-48-54.

Малыгин К. В. Проблемы вовлечения электронных данных в уголовное судопроизводство // Ex jure. 2023. № 2. С. 147–159. DOI: 10.17072/2619-0648-2023-2-147-159.

Малышева О. А. О новом векторе профессиональной подготовки следователя в условиях цифровой трансформации // Вестник Томского государственного университета. 2022. № 480. С. 262–269. DOI: 10.17223/15617793/480/29.

Маркова Т. Ю., Максимова Т. Ю. Трансформация профессиональных навыков в условиях цифровизации уголовного судопроизводства // Право и политика. 2023. № 6. С. 25–37. DOI: 10.7256/2454-0706.2023.6.40913.

Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55.

Олейник П. М., Ильин И. В., Сухов С. Н. Актуальные проблемы образовательного процесса и использования аппаратно-программных комплексов и программного обеспечения в деятельности правоохранительных органов // Вестник Нижегородского университета имени Н. И. Лобачевского. 2019. № 6. С. 157–160.

Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 450–460.

Чукова Д. И., Медведев Д. А., Литвиненко М. В. Модель формирования компетенций специалиста в сфере расследования компьютерных преступлений // Вопросы кибербезопасности. 2019. № 3 (31). С. 57–62.

Информация для цитирования

Ex jure

Моругина Н. А. Профессиональный ответ на вызовы киберпреступности: формирование кадрового потенциала для современного уголовного судопроизводства // *Ex jure*. 2026. № 3. С. 129–140. DOI: 10.17072/2619-0648-2026-3-129-140. EDN TRLTYD

Morugina N. A. Professional Response to Cybercrime Challenges: Building Human Resources for Modern Criminal Proceedings. *Ex jure*. 2026. № 3. Pp. 129–140. DOI: 10.17072/2619-0648-2026-3-129-140. EDN TRLTYD
