ISSN 2500-1442

Научная статья
УДК 343.98
EDN DPHKOC
DOI 10.17150/2500-4255.2023.17(6).586-596

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ — НОВАЯ ФОРМА ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В РАССЛЕДОВАНИИ И РАСКРЫТИИ КИБЕРПРЕСТУПЛЕНИЙ

В.Д. Пристансков[1], А.Г. Харатишвили[2], Ю.А. Евстратова[3]

[1] Санкт-Петербургский государственный университет, г. Санкт-Петербург, Российская Федерация
[2] Санкт-Петербургская академия Следственного комитета Российской Федерации, г. Санкт-Петербург, Российская Федерация
[3] Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации, г. Санкт-Петербург, Российская Федерация

Информация о статье

Дата поступления
2 октября 2023 г.

Дата принятия в печать
12 декабря 2023 г.

Дата онлайн-размещения
26 декабря 2023 г.

Ключевые слова

Искусственный интеллект; киберпреступление; преступность; специальные знания; экспертиза; машинное обучение; расследование; криминалистика; следственная деятельность; релевантный алгоритм; международная безопасность

Аннотация. В последние годы количество киберпреступлений по всему миру значительно возросло и представляет серьезную угрозу для национальной безопасности государств, информационных систем и личных данных граждан. Причиной серьезного увеличения числа киберпреступлений стало изменение мировой политики, ведение специальной военной операции, а также ограничения, обусловленные пандемией COVID-19. В научной статье рассматривается важность применения специальных знаний и искусственного интеллекта в расследовании киберпреступлений. В работе исследовано содержание понятия киберпреступления, проанализированы точки зрения ученых по решению проблем усиления противодействия указанной криминальной деятельности, имеющей в последние годы тенденцию к интенсивному распространению. В исследовании авторы приходят к выводу, что под киберпреступлениями понимается противоправное общественно опасное поведение, которое осуществляется с использованием информационных технологий и наносит существенный вред экономическим и репутационным интересам человека, организаций и государства. Дана классификация наиболее распространенных видов киберпреступлений и основных способов их совершения. Также рассмотрена научная дискуссия о содержании специальных знаний, позволившая авторам прийти к выводу, что в современных правовых условиях искусственный интеллект, как новая форма специальных знаний, требует своего осмысления в перспективе их применения в уголовном процессе. Принимая во внимание, что этот формат знаний включает в себя машинное самообучение, нейронные сети, эволюционные алгоритмы и др., предпринята попытка обосновать их применение также и для решения сложных криминалистических задач, которое требует предварительного анализа больших объемов криминалистически значимой информации, идентификации образов и закономерностей, аргументации принятия организационно-процессуальных решений. Авторами рассмотрены киберсферы, в которых используются специальные технические знания, такие как кибербезопасность, компьютерная архитектура, реверс-инжиниринг, цифровая форензика, системное администрирование. Искусственный интеллект имеет огромный потенциал в современном уголовном процессе, его использование позволит повысить эффективность следственной деятельности, так как существенно улучшит оперативность и эффективность проведения процессуальных действий и в целом досудебного производства по уголовным делам. Однако необходимо учитывать и существующие ограничения и риски, связанные с его использованием в судебно-следственной практике. Авторы приходят к выводу, что для обеспечения адекватного применения возможностей искусственного интеллекта в уголовном процессе необходимо разработать этические и правовые принципы его включения в сферу специальных знаний, используемых в уголовном судопроизводстве для формирования судебных доказательств по уголовным делам.

ISSN 2500-1442

Original article

ARTIFICIAL INTELLIGENCE — A NEW FORM OF USING SPECIAL KNOWLEDGE IN INVESTIGATINGAND SOLVING CYBERCRIMES

Vladimir D. Pristanskov[1], Anton G. Kharatishvili[2], Juliana A. Evstratova[3]
[1] *Saint Petersburg State University, Saint Petersburg, the Russian Federation*
[2] *Saint Petersburg Academy of the Investigative Committee, Saint Petersburg, the Russian Federation*
[3] *Saint Petersburg Military Order of Zhukov Institute of National Guard Troops of the Russian Federation, Saint Petersburg, the Russian Federation*

Article info
Received
2023 October 2
Accepted
2023 December 12
Available online
2023 December 26

Keywords
Artificial intelligence; cybercrime; crime; special knowledge; expertise; machine learning; investigation; criminalistics; investigative activity; relevant algorithm; international security

Abstract. The number of cybercrimes has grown considerably in recent years and now poses a serious threat for the national security of states, information systems and personal data of citizens. The reasons for this considerable increase in cybercrime are the change of global policy, the special military operation, and the restrictions connected with the COVID-19 pandemic. The authors examine the importance of using special knowledge and artificial intelligence (AI) in the investigation of cybercrimes. They research the concept of a cybercrime, and analyze the ideas of scholars on strengthening the counteraction to such criminal activities, which have been spreading rapidly in recent years. The authors conclude that cybercrimes are understood as socially dangerous unlawful behavior, carried out with the use of information technologies and inflicting considerable damage on the economic and reputational interests of people, organizations and the state. They present a classification of the most common types of cybercrimes and key methods of carrying them out. They also analyze the research discussion on the contents of special knowledge, which allows the authors to conclude that in modern legal conditions AI, being a new form of special knowledge, requires a new understanding in view of the use of this knowledge in criminal proceedings. Taking into consideration that this format includes machine self-learning, neural networks, evolutionary algorithms, etc., the authors attempt to outline how they can be used for solving complex criminalistic tasks that require a preliminary analysis of large volumes of forensically relevant information, identification of images and regularities, and argumentation of making organizational-procedural decisions. The authors examine the cyberspheres where special technical knowledge is used, such as cybersecurity, computer architecture, reverse engineering, digital forensics, system administration. AI has a tremendous potential for the modern criminal process, its use will make it possible to enhance the effectiveness of investigatory work as it will considerably improve the speed and effectiveness of procedural actions and pre-court proceedings for criminal cases in general. It is, however, necessary to take into account the existing risks and limitations connected with its use in court-investigative practice. The authors conclude that in order to ensure the adequate use of opportunities offered by AI in the criminal process, it is necessary to develop ethical and legal principles of its inclusion in the sphere of special knowledge used in criminal court proceedings for acquiring forensic evidence on criminal cases.

Современное развитие информационных технологий неизбежно повлекло трансформацию всех сфер жизни человека, общества и государства. Также это коснулось и преступности, которая всегда оперативно адаптирует в свои криминальные схемы любые современные технологии, включая и информационные, что породило новые виды общественно опасных посягательств как в границах социума, так и на глобальном уровне. Это существенно усложнило процесс противодействия преступной деятельности, приобретшей по отдельным направлениям транснациональный характер.

Апофеозом развития современных информационных технологий, несомненно, является сеть Интернет. Если провести аналогию с лекарством, когда оно может одновременно выступать и как польза, и как яд (например, при передозировке), подобная дихотомия характерна и для Интернета. Можно смело утверждать, что те возможности, которые он предоставляет (общение, обмен данными, учеба, индустрия развлечений, управление финансами и т.д.) сопоставимы с проблемами и угрозами, которые несет эта мировая сеть, имеющая доступ к информации фактически с неограниченным контентом, включая раскрытие личных (персональных)

данных, возможность совершения преступлений посредством использования интернет-ресурсов, в том числе киберпреступлений.

С ростом числа киберпреступлений по всему миру возрастает необходимость их эффективного и своевременного выявления и расследования. Традиционные (классические) организационно-тактические приемы, тактические операции и комбинации расследования в современных следственных ситуациях неэффективны. Анализ логов или обычных данных недостаточен в работе с большими данными информации (Big Date). Искусственный интеллект, с его возможностью обрабатывать и анализировать большие объемы информации, может предоставить новые тактико-технические приемы (инструменты) в борьбе с киберпреступностью.

Проблема роста количества преступлений в сфере информационных технологий по многим делам является международной. Качественная и высокоскоростная работа международных компьютерных систем, к сожалению, позволяет киберпреступникам «атаковать» законопослушных граждан из любой точки мира. Данный факт затрудняет процесс противодействия им, а именно процесс установления и привлечения криминальных субъектов к уголовной ответственности, в связи с чем возникает реальная необходимость международного сотрудничества в борьбе с киберпреступностью. Вопросы эффективного расследования киберпреступлений не раз поднимались на заседаниях ООН, Совета Европы, Интерпола, Европола. Высокая общественная опасность данных видов преступной деятельности состоит в том, что кибератаки причиняют колоссальный материальный вред как отдельным физическим и юридическим лицам, так и экономике отдельных государств и мира в целом [1, с. 77].

В апреле 2023 г. в Вене состоялась пятая сессия Специального межправительственного комитета ООН открытого состава (Спецкомитета), в рамках которой Российская Федерация выступила с инициативой создания под эгидой ООН универсального международно-правового инструмента по борьбе с киберпреступностью и предложила детализированный перечень преступлений, входящих в понятие «киберпреступность». Необходимо указать, что в Конвенции о преступности в сфере компьютерной информации, принятой в 2001 г., в ст. 2–5 были закреплены лишь четыре основных типа компьютерных преступлений[1]. В настоящее время их стало значительно больше.

Необходимо отметить, что помимо международного взаимодействия по противодействию киберпреступности назрела необходимость и на национальном уровне определить понятие киберпреступления и подготовить полноценные криминалистические методики расследования таких преступлений с использованием специальных знаний, включая их новую форму — искусственный интеллект.

В уголовно-правовой науке высказываются разные точки зрения ученых по поводу содержания понятия «киберпреступление». Так, киберпреступлениями в широком смысле признаются противоправные общественно опасные деяния, посягающие в качестве основного объекта на компьютерные системы, но также они затрагивают и дополнительные объекты, к которым отнесены: национальная и мировая безопасность (кибертерроризм), имущественные права как физических, так и юридических лиц (киберкражи, кибермошенничество), авторские права (плагиат и киберпиратство), личная безопасность (на данный объект посягательство может быть совершенно в формате таких качественно новых форм коммуникации, как кибербуллинг, секстинг, груминг, троллинг, участие в которых нередко приводит к тяжким последствиям, например к доведению до самоубийства) [2].

Думается, что под киберпреступлением целесообразно понимать противоправное общественно опасное деяние, осуществляемое с использованием информационных технологий и наносящее существенный вред интересам человека, организации, государства и общества.

Следует отметить, что криминальное киберповедение постоянно модифицируется, возникают новые виды преступной деятельности. К наиболее распространенным в настоящее время можно отнести следующие:

– кибермошенничество — реализация преступных схем обмана и злоупотребления доверием, таких, например, как фишинг, скимминг;

– киберкража — «компьютерное вторжение», включающее в себя «хакерские атаки» на компьютерные системы и сети с целью несанкционированного доступа к информации экономической направленности и незаконного перевода денежных средств;

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 : (Будапешт, 23 нояб. 2001 г.) // ИПС «Гарант».

– кибершпионаж — незаконное получение конфиденциальной (секретной) государственной либо частной информации в целях политической, экономической и военной выгоды;

– кибертерроризм — использование кибератак с целью причинения ущерба системам коммуникаций, энергетическим системам, правительственным инфраструктурам и другим особо важным государственным объектам;

– киберхулиганство — создание и распространение вредоносного программного обеспечения (вирусов, червей, троянских и других вредоносных программ) с целью причинения ущерба компьютерным системам и получения над ними контроля;

– киберэкстремизм — распространение вредоносного программного обеспечения с материалами экстремистского характера.

В современных сложных политических условиях киберпреступность постоянно эволюционирует, появляются новые изощренные криминальные способы совершения такого рода посягательств [3].

Расследование киберпреступлений невозможно без использования специальных знаний. Структура специального знания содержит собственно знания в сфере программирования и сетевых технологий и опыт в написании программ, противодействующих распространению вредоносного программного обеспечения, а также опыт в выявлении и анализе цифровых следов.

В декабре 2022 г. в докладе Александра Бастрыкина на коллегии Следственного комитета Российской Федерации было озвучено: «В 2022 году следователями расследовано свыше 15,6 тысяч деяний, совершенных с применением компьютерных технологий, что на 29 % больше, чем в 2021 году. Именно поэтому Следственный комитет активно развивает такое важное направление, как киберкриминалистика, которое повышает эффективность расследования подобных деяний»[2].

Расследование киберпреступлений в современных правовых и политических условиях требует своевременного внедрения новейших информационных технологий и их возможностей и является сложным, творческим познавательным процессом. Для успешного воссоздания преступного события необходимо привлекать экспертов и специалистов в узкоспециализированных областях научных знаний — так называемых киберзнаний.

Отличительной чертой киберпреступлений является постоянный рост «криминального профессионализма», повышенная организованность и сплоченность преступных групп, высокая латентность данного вида преступности, поскольку зачастую «жертвы» таких преступлений либо не обращаются с заявлением в правоохранительные органы по личным причинам, либо даже не подозревают о нарушении своих прав.

К вышеизложенному следует добавить нетрадиционное содержание элементов, входящих в структуру вероятностной модели, — криминалистической характеристики события киберпреступления. Криминальными субъектами разработан уникальный полноструктурный способ совершения преступлений с использованием новых IT-инструментов, таких как нейронные сети и искусственный интеллект. Криминальные субъекты используют цифровые устройства для планирования преступного поведения, осуществления и координирования своих действий. Более того, киберпреступники достаточно эффективно скрывают свою личность, используя способы цифровой маскировки IP-адресов, шифрования, прокси-серверов и т.д.

Киберпреступники широко используют автоматизированные инструменты и программы в полноструктурном способе совершения преступления, позволяющие совершать криминальные деяния в автоматическом режиме.

Место совершения преступления зачастую является нематериальным — виртуальное пространство, киберпространство. Киберпространство обладает новой, сложной характеристикой — международными связями и глобализмом. Киберпреступления не имеют границ, преступники могут находиться в одной стране, а их жертвы — в другой. Данный факт позволяет криминальным субъектам совершать кибератаки в любой точке мира, что усложняет их выявление, преследование и привлечение к ответственности.

Вышеперечисленные элементы криминалистической характеристики киберпреступлений подтверждают сложность расследования преступлений данного вида.

В этой связи следователю необходимо использовать технологии искусственного интеллекта и привлекать сведущих лиц (экспертов и специалистов) для выявления и расследования киберпреступлений.

[2] В Следственном комитете России состоялось заседание коллегии, на котором подведены итоги работы за 2022 г. URL: https://sledcom.ru/2022 год.

Необходимость привлечения сведущих лиц в уголовно-процессуальном законодательстве существовала всегда, как в монархическом, так и в советском периоде развития российской государственности[3].

Вопросы привлечения экспертов (специалистов) в уголовное судопроизводство и определения содержания понятия «специальное знание» начали активно обсуждать в конце XIX — начале XX в., однако до сих пор нет единого научного подхода к содержанию данного понятия, а также не определено место искусственного интеллекта в системе специальных знаний.

В Уголовно-процессуальном кодексе РСФСР (утвержденном Верховным Советом 27 октября 1960 г.[4]), в ст. 78, использовалось понятие «специальные познания», позже, после изменений, внесенных указом Верховного Совета РСФСР от 31 августа 1966 г.[5], в УПК РСФСР стал применяться новый термин — «специальные знания», он использовался для подтверждения квалификации и необходимых навыков специалиста, привлекаемого в уголовный процесс (ст. 133 УПК РСФСР). Термин «специальные знания» используется и в современном законодательстве — в Федеральном законе «О государственной судебно-экспертной деятельности в Российской Федерации» от 31 мая 2001 г. № 73-ФЗ (ст. 9)[6].

Как уже отмечалось, в российском уголовно-процессуальном законодательстве отсутствует определение понятия «специальные знания», несмотря на то что в дореволюционном российском уголовном процессе были установлены области специальных знаний как знаний в научной, технической, художественной или ремесленной сферах.

По данному правовому вопросу писали В.Д. Спасович [4], А.Ф. Кони [5], И.Я. Фойницкий [6], подробно раскрывал содержание специальных знаний советский профессор А.А. Эйсман [7; 8].

В правоприменительной юридической практике возникает закономерный вопрос, во-первых, о включении в содержание специальных знаний такого элемента, как опыт, наличие практических навыков и умений, во-вторых, об использовании его в профессиональной практике лица (эксперта, специалиста), в-третьих, о сфере применения специальных знаний в уголовном производстве и, в-четвертых, о возможности отнесения искусственного интеллекта к специальным знаниям.

Интересные научные изыскания по данном вопросу содержатся в трудах Ю.К. Орлова [9], Ю.Г. Корухова [10], Г.Г. Зуйкова [11], Е.И. Зуева [12], В.И. Шиканова [13].

Ю.К. Орлов считал, что специальными знаниями являются знания, которые выходят за пределы общего образования и житейского опыта и принадлежат определенной группе людей. Однако это определение спорное, так как неясно, как определить рамки житейского опыта, он индивидуален для каждого человека [9].

Ю.Г. Корухов определял специальные знания как совокупность знаний в определенной области современной науки, техники или искусства, которые используются как доказательства в уголовном деле [10].

Достаточно научно обоснованное определение, по нашему мнению, было дано В.И. Шикановым. Включая в определение рассматриваемого понятия знания из различных отраслей естественных и технических наук, различных видов искусств и ремесел, а также практический опыт и навыки, автор делает акцент на целевом назначении их применения в уголовном судопроизводстве — установление и исследование обстоятельств, подлежащих доказыванию по уголовному делу. При этом исключает из специальных общеизвестные, «которые входят в общеобразовательную подготовку граждан», а также знания из области права, связанные «с уголовно-правовой оценкой фактических обстоятельств уголовного дела и с решением процессуального характера» [13].

Указанные определения ученых не потеряли своей актуальности и в настоящее время, однако в начавшийся период активного внедрения в профессиональную деятельность цифровизации и систем искусственного интеллекта, как нам представляется, требуется расширение содержания понятия «специальные знания».

Считаем, что знания, которые не входят в классическую общеобразовательную подготовку

[3] Памятники русского права. М., 1961. Вып. 8. С. 635 ; Устав уголовного судопроизводства 1864 г. // Судебные уставы. СПб., 1867. С. 152.

[4] Уголовно-процессуальный кодекс РСФСР : утв. Верхов. Советом РСФСР 27 окт. 1960 г. // Ведомости Верховного Совета РСФСР. 1960. № 40. Ст. 592.

[5] О внесении изменений и дополнений в Уголовно-процессуальный кодекс РСФСР : указ Верхов. Совета РСФСР от 31 авг. 1966 г. // Ведомости Верховного Совета РСФСР. 1966. № 36. Ст. 1018.

[6] О государственной судебно-экспертной деятельности в Российской Федерации : федер. закон от 31 мая 2001 г. № 73-ФЗ : (ред. от 1 июля 2021 г.) // Собрание законодательства РФ. 2001. № 23. Ст. 2291.

граждан, но содержатся в поисковых интернет-системах, считаются общедоступными, и в настоящее время нецелесообразно приводить критерии разграничения общеизвестных и необщеизвестных знаний, так как наука, техника, искусство, ремесло находятся в постоянном развитии, что объясняется практической невозможностью составить перечень всех областей знаний, всех учений, теорий, наук и их отраслей, сведения из которых так или иначе отличаются от общеизвестных знаний. Тем более глобальная информатизация, которую сейчас переживают все цивилизованные страны, в том числе и Россия, оказывает существенное влияние на критерии, определяющие доступность и общеизвестность знаний.

Исследуя вышеописанные определения специальных знаний, а также определения Р.С. Белкина [14], К.А. Букалова [15], В.И. Гончаренко [16], Г.И. Грамовича [17], А.М. Зинина и Н.П. Майлис [18], В.К. Лисиченко и В.В. Циркаль [19], О.В. Евстигнеевой [20], Е.Р. Россинской и А.И. Усова [21], Н.И. Трапезниковой [22], Д.А. Харченко [23], Д.П. Чипура [24] и других ученых, мы пришли к выводу, что большинство юристов придерживаются следующей структуры специальных знаний, включающей в себя знания и опыт, в который входят навыки и умения.

Большинство определений специальных знаний в науке сводится к выделению следующих основных (в том числе и спорных) признаков знания как специального:

– система собственно знаний, навыков и умений (опыта) определенного лица (эксперта, специалиста);

– релевантность знания;

– знания в определенной области именно человеческой деятельности (науке, технике, искусстве, ремесле). Думается, что применение искусственного интеллекта, самообучающегося алгоритма — новой формы специального знания принципиально отличается от деятельности человека;

– исключение из совокупности специальных знаний правовых (в области наук уголовного профиля);

– специальные знания — это профессиональные знания (знания, полученные в результате специальной подготовки или профессионального опыта), за исключением профессиональных знаний лица, ведущего производство по делу.

Относительно рассматриваемого аспекта специальных знаний, как справедливо отмечается в литературе, они претерпевают постоянную трансформацию, поскольку, с одной стороны, знания, являвшиеся исключительной компетенцией сведущих лиц, в определенном объеме переходят в категорию общеизвестных (например, базовые знания в сфере использования средств компьютерной техники), с другой — знания правового характера, всегда относившиеся к исключительной компетенции субъекта расследования, прокурора, суда, все чаще включаются в предмет специальных знаний, поскольку современное право настолько обширно и дифференцированно, что вряд ли найдется специалист, имеющий возможность ориентироваться во всех без исключения его отраслях и институтах, особенно когда речь идет об экономических преступлениях [25].

Думается, что система специальных знаний, используемых в расследовании киберпреступлений, должна включать знания и опыт в киберсферах, к которым следует отнести:

– кибербезопасность — знание основных принципов, способов и алгоритмов обеспечения безопасности компьютерных систем, сетей и данных. Она включает знание совокупности способов защиты от вредоносных программ, криптографию, сетевую безопасность;

– компьютерную архитектуру — специальное знание о принципах работы компьютерных сетей, протоколов передачи данных и структуры сетевых систем;

– реверс-инжиниринг — аналитическое знание о вредоносном программном обеспечении (троянские программы, вирусы и другие вредоносные объекты);

– цифровую форензику — специальные знания о совокупности методов и приемов выявления, анализа и интерпретации цифровых доказательств с целью расследования киберпреступлений. Она включает цифровой поиск следов преступления в компьютерных системах, восстановление удаленных данных и анализ сетевой активности преступников;

– системное администрирование — специальные знания об управлении компьютерными системами, включая установку, настройку и обновление программного обеспечения, патч-менеджмент, мониторинг и резервное копирование данных.

Важно отметить, что борьба с киберпреступностью требует постоянного обновления знаний и осведомленности о новейших методах и угрозах.

В современных правовых реалиях встает вопрос и о релевантности, и о достоверности использования искусственного интеллекта как формы специального знания.

Применение специальных экспертных знаний и искусственного интеллекта в расследовании киберпреступлений может привести к более эффективному и точному выявлению преступных действий и предотвращению новых атак. Однако для достижения этой цели необходимо развивать не только системы и технологии, которые сочетают в себе возможности искусственного интеллекта, но и правовое основание его применения. Необходимо усиливать сотрудничество между специалистами в области кибербезопасности и разработчиками искусственного интеллекта для создания инструментов и технологий, которые могут эффективно бороться с киберпреступлениями.

Расследование киберпреступлений — это сложная и важная задача, требующая применения новой формы специальных знаний — искусственного интеллекта, но для того чтобы использовать новую форму специальных знаний, необходимо пересмотреть действующее законодательство в данной области с последующим внесением изменений и дополнений, т.е. провести его актуализацию.

Следует также особо подчеркнуть необходимость актуализации ст. 74 Уголовно-процессуального кодекса, добавив и изложив п. 3.2) в следующей редакции: «3.2) заключение специалиста с использованием технологии искусственного интеллекта и показания специалиста»[7].

Под проверяемой технологией — релевантным алгоритмом искусственного интеллекта — необходимо рассматривать алгоритм, который эффективен и применим для предварительного и судебного следствия. Он отвечает на вопросы, входящие в предмет доказывания, с высокой степенью точности и соответствия требованиям законодательства. Для того чтобы алгоритм считался релевантным, он должен обрабатывать большие объемы данных, находить закономерности, делать предсказания или принимать решения с высоким качеством и скоростью. Релевантные алгоритмы искусственного интеллекта могут включать в себя методы машинного обучения, обработки естественного языка, компьютерного зрения, робототехники и другие технологии и техники, которые позволяют системам искусственного интеллекта успешно выполнять разнообразные задачи. Оценку релевантности алгоритма в рамках уголовного процесса должен проводить эксперт (специалист).

Также считаем, что назрела необходимость включения в ст. 80 УПК РФ[8] п. 3.1 «Заключение специалиста с использованием искусственного интеллекта — представленное в письменном виде суждение по вопросам, поставленным перед специалистом сторонами, применяющим технологии искусственного интеллекта».

Считаем, что изменению подлежит и ст. 164 УПК РФ[9]. Целесообразно изложить ч. 6 в следующей редакции: «6. При производстве следственных действий могут применяться технические средства, технологии искусственного интеллекта, способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. Перед началом следственного действия следователь предупреждает лиц, участвующих в следственном действии, о применении технических средств».

Считаем, что искусственный интеллект — это новая форма современных специальных знаний, самообучаемая экспертная система, способная решать важные криминалистические задачи.

Понятие искусственного интеллекта возникло еще в 1950-х гг., но только с развитием компьютерных технологий в последние десятилетия оно получило значительное распространение и стало активно применяться в различных сферах [26].

Начало истории искусственного интеллекта связано с работами Алана Тьюринга в 1950-х гг., где он предложил Тьюринг-тест для проверки интеллектуальных способностей машины. В следующие десятилетия были созданы первые искусственные интеллектуальные системы, такие как система ШАКЕ (1973 г.) и медицинская экспертная система MYCIN (1976 г.). С развитием компьютерных технологий и объема доступных данных в современных условиях искусственный интеллект может применять компьютерное зрение, обработку естественного языка, использовать робототехнические процессы [27–29].

[7] Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 дек. 2001 г. № 174-ФЗ : (ред. от 4 авг. 2023 г.) : (с изм. и доп., вступ. в силу с 11 авг. 2023 г.) // Собрание законодательства РФ. 2001. № 52, ч. 1. Ст. 4921.

[8] Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 дек. 2001 г. № 174-ФЗ.

[9] Там же.

Искусственный интеллект включает в себя такие области знаний, как машинное самообучение, нейронные сети, эволюционные алгоритмы. Он может быть применен для решения сложных криминалистических задач, которые требуют анализа больших объемов данных, идентификации образов и закономерностей, принятия решений [30].

В Национальной стратегии развития искусственного интеллекта (2019–2030[10]) сформулированы приоритетные научные задачи, которые направлены на следующие цели: ускорение развития искусственного интеллекта в Российской Федерации, проведение научных исследований в данной области, улучшение доступности информации и вычислительных ресурсов для пользователей, а также совершенствование системы подготовки специалистов в этой сфере. Приоритетные направления развития и использования технологий искусственного интеллекта определены в России с учетом национальных целей и стратегических задач, определенных указом Президента Российской Федерации «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» от 7 мая 2018 г. № 204[11].

Искусственные нейронные сети уже продемонстрировали свою эффективность в криминалистической деятельности, они способны реализовать три типа операций: распознавание — выявление, прогнозирование, классификацию [26; 31–33].

Выявление, распознавание — установление необходимых признаков в исследуемых данных, например идентификация внешности, использование программы по автоматическому распознаванию лиц, номера автомобиля (программа «Поток»), идентификация по отпечаткам пальцев («АДИС «Папилон») [26].

Искусственный интеллект также предлагает возможность разработки прогностических моделей. Опираясь на данные о преступлениях прошлых лет, искусственный интеллект создает модели, предсказывающие вероятность возникновения преступных событий в определенных местах. Данная технология позволяет правоохранительным органам выделить более эффективные ресурсы для предотвращения преступности и борьбы с нею.

Предсказание (прогноз) — прогностическая информационная система, например программа «Форвер», используемая при построении версий.

Также существуют программы, позволяющие прогнозировать возможный процент рецидивной преступности. Искусственный интеллект выявляет корреляции и создает модели прогнозирования, которые рассчитывают вероятность повторного совершения преступления.

Прогнозирование позволяет профилировать преступника. С использованием искусственного интеллекта можно анализировать и обрабатывать данные об образе жизни, социальных связях, финансовых операциях и других факторах, связанных с преступными деяниями, чтобы выявить общие черты и особенности преступников. Данная операция используется в программе «Зеркало», разработанной А.А. Бессоновым для расследования убийств [34]. В США используется подобная система [31; 32].

Искусственный интеллект может помочь в анализе больших объемов данных, идентификации связей и паттернов, которые могут указывать на кибератаку. Системы искусственного интеллекта могут автоматически анализировать тысячи текстовых и числовых данных за короткий промежуток времени, обнаруживать аномалии и подозрительные действия.

Дешифрование и кодирование часто являются сложными задачами в расследовании преступлений. Использование искусственного интеллекта, в частности нейронных сетей, позволяет автоматизировать процесс расшифровки, дешифрирования и анализа данных, таких как шифрованные сообщения или файлы. Данная технология значительно ускоряет процесс расследования.

Нейронные сети — модель компьютерного обучения, позволяющая обрабатывать сложные и неструктурированные данные, такие как изображения, звук, текст и видео. Применение нейронных сетей в расследовании киберпреступлений может повысить точность обнаружения аномалий и идентификацию потенциальных угроз.

Машинное обучение в расследовании киберпреступлений может быть использовано для

[10] О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) : указ Президента РФ от 10 окт. 2019 г. № 490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

[11] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : указ Президента РФ от 7 мая 2018 г. № 204 // Собрание законодательства РФ. 2018. № 20. Ст. 2817.

создания моделей, способных обнаруживать и классифицировать различные типы киберпреступлений. Благодаря искусственному интеллекту разрабатываются и совершенствуются инновационные системы обнаружения IT-способов совершения преступлений, которые могут автоматически обнаруживать и блокировать подозрительную криминальную активность субъекта в режиме реального времени. Данные системы основаны на алгоритмах машинного обучения, которые позволяют искусственному интеллекту непрерывно повышать эффективность защиты от киберугроз. Кроме того, искусственный интеллект дает возможность разрабатывать уникальные криптографические алгоритмы, обеспечивающие безопасность и защиту информации от взломов, что позволяет создавать надежные системы шифрования.

Системы учета (классификаторы) разрабатываются в борьбе с терроризмом и экстремизмом и уже применяются в отдельных тактических операциях, реализуемых правоохранительными органами Российской Федерации и за рубежом [26; 35; 36].

Резюмируя вышеизложенное, считаем, что в настоящее время назрела необходимость на законодательном уровне закрепить содержание понятия «специальные знания» и подготовить нормативно-правовую базу для новой формы специальных знаний — искусственного интеллекта, используемого в следственной деятельности. Искусственный интеллект имеет огромный потенциал в повышении эффективности деятельности следователя, экспертов и специалистов в рамках расследуемого уголовного дела. Применение искусственного интеллекта позволяет повысить качество и оптимизировать сроки расследования. Однако необходимо также учитывать ограничения и риски, связанные с использованием искусственного интеллекта, и обеспечить этическое и юридическое регулирование его применения в уголовном процессе.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия / Г.В. Семеко. — DOI 10.31249/snsn/2020.01.06. — EDN ANGCNJ // Социальные новации и социальные науки. — 2020. — № 1 — С. 77–96.

2. Мирончик А.С. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации / А.С. Мирончик, А.В. Суслопаров. — DOI 10.25136/2409-7136.2019.9.30745. — EDN ONIEJG // Юридические исследования. — 2019. — № 9. — С. 17–30.

3. Клишков В.Б. Киберпреступность: понятие, признаки, основные направления противодействия / В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева. — DOI 10.52452/19931778_2022_4_106. — EDN WWFAEM // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2022. — № 4. — С. 106–114.

4. Спасович В.Д. О теории судебно-уголовных доказательств в связи с судоустройством и судопроизводством / В.Д. Спасович. — Москва : ЛексЭст, 2001. — 93 с.

5. Кони А.Ф. Избранное / А.Ф. Кони. — Москва : Сов. Россия, 1989. — 495 с.

6. Фойницкий И.Я. Курс уголовного судопроизводства. В 2 т. Т. 2 / И.Я. Фойницкий. — Санкт-Петербург : Альфа, 1996. — 607 с.

7. Эйсман А.А. Заключение эксперта: структура и научные обоснования / А.А. Эйсман. — Москва : Юрид. лит., 1967. — 152 с.

8. Эйсман А.А. Критерии и формы использования специальных познаний при криминалистическом исследовании в целях получения судебных доказательств / А.А. Эйсман // Вопросы криминалистики. — 1962. — № 6. — С. 33–45.

9. Орлов Ю.К. Заключение эксперта и его оценка по уголовным делам / Ю.К. Орлов. — Москва : Юрист, 1995. — 64 с.

10. Корухов Ю.Г. Правовые основы применения научно-технических средств при расследовании преступлений / Ю.Г. Корухов. — Москва, 1974. — 29 с.

11. Зуйков Г.Г. Общие вопросы использования специальных познаний в процессе предварительного расследования / Г.Г. Зуйков // Криминалистическая экспертиза / под общ. ред. Р.С. Белкина, И.М. Лузгина. — Москва, 1956. — Вып. 1. — С. 113–125.

12. Зуев Е.И. Непроцессуальная помощь сотрудника криминалистического подразделения следователю / Е.И. Зуев. — Москва, 1975. — 39 с.

13. Шиканов В.И. Использование специальных познаний при расследовании убийств : учеб. пособие / В.И. Шиканов. — Иркутск, 1976. — 88 с.

14. Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. — Москва : Мегатрон-XXI, 2000. — 333 с.

15. Букалов К.А. Применение товароведческих познаний при проведении комплексной ревизии по требованию следователя / К.А. Букалов // Теория и практика криминалистики и судебной экспертизы. — Саратов, 1982. — Вып. 4. — С. 90.

16. Гончаренко В.И. Использование данных естественных и технических наук в уголовном судопроизводстве: (методологические вопросы) / В.И. Гончаренко. — Киев, 1980. — 157 с.

17. Грамович Г.И. Тактика использования специальных знаний в раскрытии и расследовании преступлений : учеб. пособие / Г.И. Грамович. — Минск, 1987. — 66 с.

18. Зинин А.М. Судебная экспертиза : учебник / А.М. Зинин, Н.П. Майлис. — Москва : Юрайт, 2002. — 318 с.

19. Лисиченко В.К. Использование специальных знаний в следственной и судебной практике : учеб. пособие / В.К. Лисиченко, В.В. Циркаль. — Киев : Киев. гос. ун-т им. Т.Г. Шевченко, 1987. — 100 с.

20. Евстигнеева О.В. Использование специальных познаний в доказывании на предварительном следствии в российском уголовном процессе : дис. … канд. юрид. наук : 12.00.09 / О.В. Евстигнеева. — Саратов, 1998. — 194 с.

21. Россинская Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. — Москва : Право и закон, 2001. — 416 с. — EDN TSBNDF.

22. Трапезникова И.И. Специальные знания в уголовном процессе России: понятие, признаки, структура : автореф. дис. … канд. юрид. наук : 12.00.09 / И.И. Трапезникова. — Челябинск, 2004. — 22 с.

23. Харченко Д.А. Судебная экспертиза в российском уголовном судопроизводстве : автореф. дис. … канд. юрид. наук : 12.00.09 / Д.А. Харченко. — Иркутск, 2006. — 22 с.

24. Чипура Д.П. Использование специальных экономических знаний при расследовании преступлений : автореф. дис. … канд. юрид. наук : 12.00.09 / Д.П. Чипура. — Волгоград, 2005. — 20 с.

25. Специальные знания в уголовном судопроизводстве : хрестоматия / Е.В. Елагина, Т.Г. Николаева, Н.А. Данилова. — Санкт-Петербург, 2022. — 204 с.

26. Степаненко Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Д.В. Бахтеев, Ю.А. Евстратова. — DOI 10.17150/2500-4255.2020.14(2).206-214. — EDN FDCVTB // Всероссийский криминологический журнал. — 2020. — Т. 14, № 2. — С. 206–214.

27. Рассел С. Искусственный интеллект. Современный подход / С. Рассел, П. Норвиг. — 2-е изд. — Москва : Вильямс, 2018. — 1408 с.

28. Haugeland J. Artificial Intelligence: The Very Idea / J. Haugeland. — Cambridge : MIT Press, 1981. — 287 p.

29. Bellman R. An Introduction to Artificial Intelligence: Can Computers Think? / R. Bellman. — San Francisco : Boyd and Fraser Publishing Company, 1978. — 146 p.

30. Финн В.К. Искусственный интеллект: Методология, применения, философия / В.К. Финн ; ред. М.А. Михеенкова. — Москва : Красанд, 2018. — 436 с.

31. Rich E. Artificial Intelligence / E. Rich, K. Knight. — 2nd ed. — New York : McGraw-Hill, 1991. — 621 p.

32. Charniak E. Introduction to Artificial Intelligence / E. Charniak, D. McDermott. — Reading : Addison-Wesley, 1985. — 701 p.

33. Nilsson N.J. Artificial Intelligence: A New Synthesis / N.J. Nilsson. — San Francisco : Morgan Kaufmann, 1998. — 513 p.

34. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений / А.А. Бессонов. — Москва : Проспект, 2021. — 816 с. — EDN PNSDMT.

35. Бахтеев Д.В. Причинность и случайность как объекты восприятия в структуре криминалистического мышления / Д.В. Бахтеев. — DOI 10.17150/2500-4255.2019.13(2).252-261. — EDN VLAPDN // Всероссийский криминологический журнал. — 2019. — Т. 13, № 2. — С. 252–261.

36. Rockwell L.R. Forensic Intelligence Analysis / L.R. Rockwell // Encyclopedia of Forensic Sciences. — 2nd ed. — San Diego, 2013. — Vol. 3. — P. 341–345.

REFERENCES

1. Semeko G.V. Information Security in the Financial Sector: Cybercrime and Counteraction Strategies. *Sotsial'nye novatsii i sotsial'nye nauki = Social Novelties and Social Sciences*, 2020, no. 1, pp. 77–96. (In Russian). EDN: ANGCNJ. DOI: 10.31249/snsn/2020.01.06.

2. Mironchik A.S., Susloparov A.V. Electronic Theft as a Kind of Computer Crime: Problems that Arise during Differentiation and Qualification of This Kind of Crime. *Yuridicheskie issledovaniya = Legal Studies*, 2019, no. 9, pp. 17–30. (In Russian). EDN: ONIEJG. DOI: 10.25136/2409-7136.2019.9.30745.

3. Klishkov V.B., Stebeneva E.V., Yakovleva M.A. Cybercrime: Concept, Signs, Main Directions of Counteraction. *Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo = Vestnik of Lobachevsky University of Nizhnii Novgorod*, 2022, no. 4, pp. 106–114. (In Russian). EDN: WWFAEM. DOI: 10.52452/19931778_2022_4_106.

4. Spasovich V.D. *On the Theory of Court-Criminal Proof in Connection with the Organization of Courts and Court Proceedings.* Moscow, LeksEst Publ., 2001. 93 p.

5. Koni A.F. *Selected Works*. Moscow, Sovetskaya Rossiya Publ., 1989. 465 p.

6. Foinitskii I.Ya. *The Course of Criminal Proceedings*. Saint Petersburg, Alfa Publ.,1996. Vol. 2. 607 p.

7. Eisman A.A. *An Expert's Verdict: Structure and Scientific Grounds.* Moscow, Yuridicheskaya Literatura Publ., 1967. 152 p.

8. Eisman A.A. Criteria and Forms of Using Special Knowledge in Criminalistic Examination with the Purpose of Obtaining Court Evidence. *Voprosy kriminalistiki = Issues of Criminalistics*, 1962, no. 6, pp. 33–45. (In Russian).

9. Orlov Yu.K. *Expert Opinion and Assessment in Criminal Cases*. Moscow, Yurist Publ., 1995. 64 p.

10. Korukhov Yu.G. *Legal Basis of Using Technical Equipment in Crime Investigation.* Moscow, 1974. 29 p.

11. Zuikov G.G. General Questions of Using Special Knowledge in the Process of Preliminary Investigation. In Belkin R.S., Luzgin I.M. (eds.). *Criminalistic Expertise.* Moscow, 1956. Iss. 1, pp. 113–125. (In Russian).

12. Zuev E.I. *Non-procedural Assistance to the Investigator Provided by a Criminalistic Department Representative.* Moscow, 1975. 39 p.

13. Shikanov V.I. *Use of Special Knowledge in Investigating Murders.* Irkutsk, 1976. 88 p.

14. Belkin R.S. *Criminalistic Encyclopedia.* Moscow, Megatron-XXI Publ., 2000. 333 p.

15. Bukalov K.A. The Use of Merchandise-related Knowledge during a Complex Audit at the Request of the Investigator. *The Theory and Practice of Criminalistics and Forensic Examination*. Saratov, 1982. Iss. 8, pp. 90. (In Russian).

16. Goncharenko V.I. *The Use of Data from Natural and Technical Sciences in Criminal Proceedings (Questions of Methodology).* Kiev, 1980. 157 p.

17. Gramovich G.I. *The Tactics of Using Special Knowledge in Investigating and Solving Crimes.* Minsk, 1987. 66 p.

18. Zinin A.M., Mailis N.P. *Forensic Examination.* Moscow, Yurait Publ., 2002. 318 p.

19. Lisichenko V.K. *The Use of Special Knowledge in Investigation and Court Practice.* Taras Shevchenko National University of Kyiv Publ., 1987. 100 p.

20. Evstigneeva O.V. *The Use of Special Knowledge in Proving during Preliminary Investigation in Russian Criminal Process. Cand. Diss*. Saratov, 1998. 194 p.

21. Rossinskaya E.R., Usov A.I. *Judicial Computer-Technical Expertise*. Moscow, Pravo i Zakon Publ., 2001. 416 p. EDN: TSBNDF.

22. Trapeznikova I.I. *Special Knowledge in Russian Criminal Process: Concept, Features, Structure. Cand. Diss. Thesis*. Chelyabinsk, 2004. 22 p.

23. Kharchenko D.A. *Forensic Expertise in Russian Criminal Proceedings. Cand. Diss. Thesis*. Irkutsk, 2006. 22 p.

24. Chipura D.P. *The Use of Special Economic Knowledge in Crime Investigation. Cand. Diss. Thesis*. Volgograd, 2005. 20 p.

25. Elagina E.V., Nikolaeva T.G., Danilova N.A. *Special Knowledge in Criminal Court Proceedings.* Saint Petersburg, 2022. 204 p.

26. Stepanenko D.A., Bakhteev D.V., Evstratova Yu.A. The Use of Artificial Intelligence Systems in Law Enforcement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 2, pp. 206–214. (In Russian). EDN: FDCVTB. DOI: 10.17150/2500-4255.2020.14(2).206-214.

27. Russell S.J. Norvig P. *Artificial Intelligence. A Modern Approach.* Noida, India, Pearson India Education Services Pvt. Ltd., 2015. 1145 p. (Russ. ed.: Russell S.J., Norvig P. *Artificial Intelligence. A Modern Approach.* Moscow, Williams Publ., 2018. 1408 p.).

28. Haugeland J. *Artificial Intelligence: The Very Idea*. Cambridge, MIT Press, 1981. 287 p.

29. Bellman R. *An Introduction to Artificial Intelligence: Can Computers Think*? San Francisco, Boyd and Fraser Publishing Company, 1978. 146 p.

30. Finn V.K. *Artificial Intelligence: Methodology, Applications, Philosophy*. Moscow, Krasand Publ., 2018. 436 p.

31. Rich E., Knight K. *Artificial Intelligence*. 2nd ed. New York, McGraw-Hill, 1991. 621 p.

32. Charniak E., McDermott D. *Introduction to Artificial Intelligence.* Reading, Addison-Wesley, 1985. 701 p.

33. Nilsson N.J. *Artificial Intelligence: A New Synthesis*. San Francisco, Morgan Kaufmann, 1998. 513 p.

34. Bessonov A.A. *Artificial Intelligence and Mathematical Statistics in the Criminalistic Study of Crimes.* Moscow, Prospekt Publ., 2021. 816 p. EDN: PNSDMT.

35. Bakhteev D.V. Causality and Randomness as Objects of Perception in the Structure of Criminalistic Thinking. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 2, pp. 252–261. (In Russian). EDN: VLAPDN. DOI: 10.17150/2500-4255.2019.13(2).252-261.

36. Rockwell L.R. Forensic Intelligence Analysis. *Encyclopedia of Forensic Sciences*. 2nd ed. San Diego, 2013. Vol. 3, pp. 341–345.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Пристансков Владимир Дмитриевич — и.о. заведующего кафедрой уголовного процесса и криминалистики Санкт-Петербургского государственного университета, кандидат юридических наук, профессор, г. Санкт-Петербург, Российская Федерация; e-mail: vdpristanskov@mail.ru.

Харатишвили Антон Георгиевич — заведующий кафедрой уголовного процесса Санкт-Петербургской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент, г. Санкт-Петербург, Российская Федерация; e-mail: dashuta2003@yandex.ru.

Евстратова Юлиана Айратовна — заведующий кафедрой философских и социально-экономических дисциплин Санкт-Петербургского военного ордена Жукова института войск национальной гвардии Российской Федерации, кандидат юридических наук, доцент, г. Санкт-Петербург, Российская Федерация; e-mail: yuliana130682@mail.ru.

INFORMATION ABOUT THE AUTHOR

Pristanskov, Vladimir D. — Acting Head, Department of Criminal Procedure and Criminalistics, Saint Petersburg State University, Ph.D. in Law, Professor, Saint Petersburg, the Russian Federation; e-mail: vdpristanskov@mail.ru.

Kharatishvili, Anton G. — Head, Department of Criminal Procedure, Saint Petersburg Academy of the Investigative Committee of the Russian Federation, Ph.D. in Law, Ass. Professor, Saint Petersburg, the Russian Federation; e-mail: dashuta2003@yandex.ru.

Evstratova, Juliana A. — Head, Department of Philosophical and Socio-Economic Disciplines, Saint Petersburg Military Order of Zhukov Institute of the National Guard of the Russian Federation, Ph.D. in Law, Ass. Professor, Saint Petersburg, the Russian Federation; e-mail: yuliana130682@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Пристансков В.Д. Искусственный интеллект — новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений / В.Д. Пристансков, А.Г. Харатишвили, Ю.А. Евстратова. — DOI 10.17150/2500-4255.2023.17(6).586-596. — EDN DPHKOC // Всероссийский криминологический журнал. — 2023. — Т. 17, № 6. — С. 586–596.

FOR CITATION

Pristanskov V.D., Kharatishvili A.G., Evstratova Ju.A. Artificial Intelligence — a New Form of Using Special Knowledge in Investigating and Solving Cybercrimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 6, pp. 586–596. (In Russian). EDN: DPHKOC. DOI: 10.17150/2500-4255.2023.17(6).586-596.