Дата поступления рукописи в редакцию: 20.03.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-43-44

АРИПШЕВ Ахмед Мухамедович,
заместитель начальника кафедры огневой подготовки,
кандидат экономических наук, полковник полиции,
e-mail: mail@law-books.ru

ОБЩЕТЕОРЕТИЧЕСКИЕ, ПСИХОЛОГИЧЕСКИЕ И ИНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. *Для повышения эффективности противодействия киберпреступности необходим комплексный, опережающий подход, сочетающий правовые, организационные и технологические меры. Автор с исследовании отмечает, что первоочередной мерой является совершенствование уголовного и процессуального законодательства путем криминализации новых способов совершения преступлений: целесообразно ввести отдельные составы, учитывающие использование AI и глубоких подделок для мошенничества, шантажа и манипуляции общественным мнением. Необходима унификация понятийного аппарата через закрепление на законодательном уровне четкого определения киберпреступления, созвучного с международными подходами.*

Ключевые слова: *уголовное и процессуальное законодательство, новые способы совершения преступлений, использование AI, мошенничество, унификация понятийного аппарата, киберпреступления.*

ARIPSHEV Ahmed Mukhamedovich,
Deputy Head of the Department of Fire Training,
Candidate of Economic Sciences, Police Colonel

GENERAL THEORETICAL, PSYCHOLOGICAL AND OTHER ISSUES OF COUNTERING EXTREMISM AND TERRORISM IN MODERN CONDITIONS

Annotation. *To improve the effectiveness of countering cybercrime, a comprehensive, proactive approach is needed, combining legal, organizational, and technological measures. The author notes in his study that the primary measure is to improve criminal and procedural legislation by criminalizing new methods of committing crimes: it is advisable to introduce separate offenses that take into account the use of AI and deepfakes for fraud, blackmail, and manipulation of public opinion. Unification of the conceptual framework is necessary by enshrining in law a clear definition of cybercrime consistent with international approaches.*

Key words: *criminal and procedural legislation, new methods of committing crimes, use of AI, fraud, unification of the conceptual framework, cybercrime.*

Противодействие киберпреступности в цифровую эпоху является одной из наиболее сложных и актуальных задач для обеспечения национальной и международной безопасности. Проведенное исследование позволяет констатировать, что существующая в России система мер, несмотря на ее постоянное развитие, все еще отстает от динамично меняющихся киберугроз. Ключевыми проблемами остаются архаичность уголовного законодательства, сложности с квалификацией и доказыванием, кадровый дефицит и недостаточный уровень международной кооперации.

Для кардинального изменения ситуации необходим переход к опережающей модели уголовной политики, основанной на глубокой интеграции правовых, организационных и технологических мер.

Проведённое исследование позволяет констатировать, что конкуренция уголовно-правовых норм при квалификации насильственных преступлений представляет собой устойчивую и системную проблему современной уголовно-правовой практики. Специфика обусловлена высокой степенью нормативной дифференциации составов преступлений против личности, нали-

чием многочисленных квалифицирующих признаков, а также использованием оценочных категорий, наполняемых содержанием преимущественно через судебную практику [2].

Анализ научных публикаций 2022–2026 гг. и судебных решений за указанный период подтверждает отсутствие единообразия при разграничении смежных составов преступлений. Наиболее сложными остаются вопросы соотношения общей и специальной нормы, части и целого, а также разграничения конкуренции норм и совокупности преступлений. Практика демонстрирует случаи как избыточной инкриминации, когда содеянное необоснованно квалифицируется по нескольким статьям, так и неполной уголовно-правовой оценки, при которой отдельные признаки преступления «поглощаются» без достаточных оснований.

В условиях стремительной цифровизации преступности, традиционные формы мониторинга сети Интернет участниками общественных объединений посредствам ручного поиска остаются низко эффективными.

Современный этап характеризуется переходом кибердружин к использованию автоматизированных систем на базе искусственных нейронных сетей. В современной цифровой среде общественные объединения правоохранительной направленности сталкиваются с проблемой намеренного искажения лексики и использования специфического сленга для обхода автоматических систем фильтрации.

Особую значимость приобретает использование возможностей искусственного интеллекта в деятельности кибердружин по противодействию наркопреступности в цифровой среде. Современные системы на базе искусственного интеллекта способны распознавать скрытую рекламу наркотиков, анализируя контекст и структуру сообщения. Нейросеть обучается распознавать намеренные искажения слов, замену букв цифрами, использование иных символов и изображений вместо названий веществ, что раньше было главным способом обхода фильтров [3].

Внедрение искусственного интеллекта в деятельность общественных объединений правоохранительной направленности радикально меняет инструментарий участия граждан в обеспечении правопорядка. Переход от пассивного наблюдения к упреждающему наблюдению и значительно повышает эффективность предупреждения правонарушений на ранних стадиях. Несмотря на высокий потенциал, широкое применение искусственного интеллекта общественниками сопряжено с серьезными рисками. В частности, выявлена необходимость четкого законодательного регулирования.

В заключение отметим, что искусственный интеллект должен рассматриваться не как замена человеческому участию, а как инструмент интеллектуальной поддержки, позволяющий общественным объединениям действовать более прицельно и эффективно.

Комплексное использование гражданской инициативы и высоких технологий способно создать принципиально новую модель общественной безопасности, основанную на прозрачности, скорости реакции и предупредительном подходе.

Список литературы:

[1] Безгачев Ф. В. Применение искусственного интеллекта (нейронных сетей) в деятельности полиции // Закон и власть. 2023. №3. URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-neyronnyh-setey-v-deyatelnosti-politsii (дата обращения: 06.05.2026).

[2] Карпика А. Г. Анализ направлений применения искусственного интеллекта в правоохранительной деятельности // ЮП. 2023. №1 (104). URL: https://cyberleninka.ru/article/n/analiz-napravleniy-primeneniya-iskusstvennogo-intellekta-v-pravo-ohranitelnoy-deyatelnosti (дата обращения: 06.05.2026).

[3] Машекуашева М.Х. Вопросы эффективности борьбы с интернет-мошенничеством: повышение результативности функционирования правоохранительных органов. Экономика и право. XXI век. 2025. № 2. С. 43-44.

References:

[1] Bezgachev F.V. Application of artificial intelligence (neural networks) in police activities// Law and power. 2023. №3. URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-neyronnyh-setey-v-deyatelnosti-politsii (дата обращения: 06.05.2026).

[2] Karpika A. G. Analysis of the areas of application of artificial intelligence in law enforcement// UP. 2023. №1 (104). URL: https://cyberleninka.ru/article/n/analiz-napravleniy-primeneniya-iskusstvennogo-intellekta-v-pravoohranitelnoy-deyatelnosti (дата обращения: 06.05.2026).

[3] Mashekuasheva M.Kh. Issues of the effectiveness of combating Internet fraud: increasing the effectiveness of the functioning of law enforcement agencies. Economics and law. XXI century. 2025. № 2. S. 43-44.