

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В КРИМИНАЛИСТИКЕ НА ПРИМЕРЕ ПРОТИВОДЕЙСТВИЯ ВЫСОКОТЕХНОЛОГИЧНОЙ ПРЕСТУПНОСТИ

Поляков Вит.В.¹, Милич И.Д.²

*¹ Алтайский государственный университет, г. Барнаул
e-mail: agipolyakov@gmail.com*

*² Юридический факультет государственного Университета в городе Нови-Сад, Республика Сербия, г. Нови-Сад
e-mail: i.milic@pf.uns.ac.rs*

Аннотация. С криминалистических позиций исследованы перспективы применения методов машинного обучения и «усиленного интеллекта» в противодействии высокотехнологичной преступности. Для этого проанализированы особенности современной преступности, реализующей методы машинного обучения, в частности, отмечено появление новых видов и разновидностей преступлений в сфере компьютерной информации, связанных с использованием методов машинного обучения. Выявляемые закономерности и особенности предлагается обобщить и отразить в соответствующих криминалистических характеристиках преступлений, а также в формировании типовых криминальных ситуаций. Обоснована необходимость разработки новой методологии расследования преступлений, основанной на использовании методов машинного обучения и систем, использующих алгоритмы «усиленного интеллекта». На базе такой методологии должна быть проведена разработка общих криминалистических технических, тактических и методических подходов по расследованию преступлений. Отмечено, что одной из первых прикладных форм реализации данных технологий может стать экспертная практика. Особенно перспективным представляется применение методов машинного обучения и систем «усиленного интеллекта» при решении задач, нацеленных на предупреждение преступлений, в частности, за счет комбинированного использования в исследовательских системах honeypot.

Ключевые слова: машинное обучение, «усиленный интеллект», высокотехнологичные преступления, криминалистическая методология, объект криминалистики

Стремительный прогресс информационных технологий в конце XX – начале XXI века привел к появлению такого принципиально нового явления, как компьютерные системы, объединяемые понятием искусственного интеллекта. В то же время, несмотря на широкое использование этого понятия в правовых научных исследованиях, сколько-нибудь единого и общепризнанного определения термина «искусственный интеллект» не существует. В силу этого расширяющееся применение данного понятия без попытки его формального определения представляется малопродуктивным, разные авторы вкладывают в него совершенно различное и достаточно «размытое» содержание. Полагаем, что в настоящее время при криминалистических исследованиях правильнее говорить скорее о так называемом «усиленном интеллекте» (machine augmented intelligenc) [1, с. 278]. Его выражением являются информационные системы, представляющие собой самообучающиеся компьютерные программы. Работа этих программ основана на использовании математических алгоритмов машинного обучения.

Для применения методов машинного обучения в криминалистике необходимо наличие достаточно больших статистических выборок [2, с. 11-17], [3, с. 54-70], включающих информацию об обстоятельствах преступлений определенного вида и

типовых и типичных ситуациях, формировавшихся при проведении их расследования (другими словами, криминалистически значимую информацию [4, с. 237]. В результате самообучения компьютерной программы по массивам этих данных появляются такие важные возможности, как, во-первых, выявление скрытых (латентных) закономерностей, не обнаруживаемых традиционными способами анализа [5]. Во-вторых, в результате работы обучившейся программы для расследуемого преступления могут быть предложены оптимальные способы разрешения конкретной криминалистической ситуации, то есть оптимальные методы и тактические приемы криминалистических действий. Такое применение машинного обучения обеспечивает, используя выражение В.Б. Вехова, «разработку автоматизированных методик расследования преступлений» [6, с. 635], относимое им к одному из инновационных направлений развития криминалистики.

Отметим, что актуальность применения методов машинного обучения в криминалистике существенно усиливается вследствие возрастающего давления нового негативного фактора. Этим фактором являются усиливающиеся попытки организованных преступных групп привлекать подобные методы [7, с. 38]. прежде всего при совершении высокотехнологичных преступлений [8], а также современных разновидностей терроризма [9], мошенничества [10]. Такая тенденция в развитии высокотехнологичной преступности требует разработки и апробации принципиально новых технических, тактических и методических рекомендаций по расследованию преступлений.

Анализ сложившихся к настоящему времени тенденций по использованию информационных систем с элементами машинного обучения в уголовном судопроизводстве показал, что это использование отвечает, как правило, следующим направлениям:

- алгоритмизация процесса расследования;
- применение при проведении экспертных исследований, прежде всего компьютерно-технических экспертиз [11];
- поисково-идентификационные задачи в рамках оперативно-розыскной деятельности [2];
- предупреждения совершения преступлений (распознавание признаков готовящихся преступлений и т.п.).

В этом смысле полагаем, что возможности методов машинного обучения шире, чем отмеченные в работе Д.А. Степаненко, Д.В. Бахтеева, Ю.А. Евстратова, выделивших «... три основных типа операций в сфере правоохранительной деятельности, которые могут быть разрешены посредством использования систем искусственного интеллекта: распознавание (визуальных образов и связей между объектами криминалистического познания), предсказание и классификация» [12].

На наш взгляд, для успешного внедрения технологий машинного обучения в современную отечественную криминалистическую деятельность необходимы следующие меры.

1. Изучение передового отечественного и зарубежного опыта использования методов машинного обучения в различных областях деятельности с целью адаптации к задачам противодействия преступности, прежде всего высокотехнологичной [13, 14, 15, с. 114-125].

2. Радикальное улучшение правовых и организационных механизмов взаимодействия с зарубежными правоохранительными органами в борьбе с трансграничной [16] преступностью, использующей передовые информационные технологии, например, высокотехнологичной преступности. Как справедливо отметил В.Б. Батоев, в современных сложных геополитических условиях «...сформированные «барьеры» привели к недопониманию в вопросах оказания взаимной правовой помощи; обмена информацией, опытом противодействия

киберпреступности, технологическими новинками, разработками и передовыми техническими решениями в сфере информационно-телекоммуникационных технологий» [2].

3. Разработка новых методологических подходов к раскрытию и расследованию преступных деяний, которые совершаются с использованием методов машинного обучения («усиленного интеллекта»). Заметим, что данная методология может быть распространена на противодействие традиционной преступности.

4. Повышение потенциала экспертных исследований на основе привлечения методов машинного обучения, прежде всего к проведению компьютерно-технических экспертиз.

5. Изучение с помощью машинного обучения криминогенных объектов, наиболее уязвимых для преступных посягательств с использованием удаленного доступа по информационным сетям, и разработка мер криминалистического предупреждения совершения данных преступлений [5, 17].

Исходя из приведенных перспективных направлений, рассмотрим более подробно те из них, которые, по нашему мнению, требуют первоочередного развития.

1. Необходимо изучить изменения в современной высокотехнологичной преступности, проявляющиеся в активном использовании находящегося в свободном доступе или слабо защищенного компьютерного программного обеспечения, реализующего методы машинного обучения. Другими словами, компьютерные программы, построенные на принципах машинного обучения, становятся, с одной стороны, предметом преступных посягательств, а с другой - специфическим средством совершения преступлений.

Проявлением отмеченных изменений в преступности является внедрение в криминальную деятельность новых технологических возможностей (информационных и коммуникационных), основанных на применении методов машинного обучения и программных алгоритмов, близких к ним по своему действию, при совершении традиционных видов преступлений. В качестве примера можно привести мошенничество, когда один модуль программы, работающий на методах машинного обучения, собирает информационные данные о потенциальных жертвах, а второй модуль (так называемый чат-бот) осуществляет первичный автоматизированный контакт с отобранными жертвами для сбора конфиденциальной информации.

Следует также отметить появление новых видов и разновидностей преступлений в сфере компьютерной информации, связанных с использованием методов машинного обучения. Так, например, новые разновидности компьютерных вирусов обладают некоторыми признаками самоорганизации, адаптируясь к различным условиям для более успешного внедрения в защищенные компьютерные системы. В частности, они могут осуществлять избирательную маскировку под доверенное программное обеспечение. Некоторые вредоносные программы получили возможность самовоспроизводства с новыми функциями и возможностями [7, с. 38].

2. Описанные изменения в способах совершения высокотехнологичных преступлений, связанные с использованием методов машинного обучения, ставят перед криминалистикой актуальную задачу обобщения криминалистически значимых закономерностей и выявления специфических особенностей этих преступлений. Эти закономерности и особенности должны найти отражение в соответствующих криминалистических характеристиках [18, с. 52, 19, 20, с. 36], а также в формировании типовых криминальных ситуаций [21 - 25]. Заметим, что описывать прогнозируемые способы совершения таких преступлений следует

крайне осторожно, так как это может спровоцировать потенциальных преступников как «руководство к действию».

3. Необходимо разработать новую методологию расследования преступлений, основанную на использовании методов машинного обучения и систем, использующих алгоритмы «усиленного интеллекта». Полагаем, что на сегодняшний день это одно из наиболее актуальных новых направлений в криминалистике, имеющее различные пути реализации. Возможности и полезная роль алгоритмизации работы следователя исследуются в криминалистике достаточно давно [26 - 28], но именно использование методов машинного обучения способно уже в ближайшее время придать этим положениям качественно новый уровень. В числе основных задач, которые могут решаться для внедрения в правоохранительную деятельность методов машинного обучения, видятся следующие:

- формирование статистически достаточных выборок для машинного обучения [29, 30], полученных, в частности, в результате выделения судебно-следственных ситуаций, складывающихся при расследовании преступлений;
- разработка алгоритмов машинного обучения, адаптированных непосредственно под задачи уголовного судопроизводства [31, с. 176].

4. На базе новой методологии может быть проведена разработка общих криминалистических технических и тактических подходов, а также методов, приемов, рекомендаций и частных методик по расследованию преступлений.

В результате могут быть построены ретроспективные и перспективные версии, содержащие рекомендации для оптимальных направлений расследования в различных ситуациях расследования. Различного рода программы и системы, использующие методы машинного обучения, смогут помочь в организации и алгоритмизации процесса производства по уголовным делам на досудебных и судебных стадиях [32].

Отметим, что новые криминалистические средства, в основу которых положены принципы машинного обучения («усиленного интеллекта»), в настоящее время могут использоваться только в качестве оперативной и ориентирующей информации [33]. Это обусловлено, в первую очередь, отсутствием необходимой правовой регламентации применения таких технологий в правоохранительной деятельности и опыта их использования в уголовном судопроизводстве.

5. Внедрение методов машинного обучения в экспертную деятельность (например, распознавание и сравнение образов в идентификационных задачах, выявление качеств в диагностических задачах, классифицирование по заданным параметрам эмпирических данных и т.д.) позволит обрабатывать значительные объемы информации, открывая широкие перспективы в решении вопросов, ранее невыполнимых или требующих сложной реализации [34]. Кроме того, способность методов машинного обучения (многомерного анализа данных, нейронных сетей и т.п.) к обучению на основе вновь получаемой информации способно снижать вероятность ошибок и упущений при проведении судебных экспертиз.

6. Особенно перспективным представляется применение методов машинного обучения и систем «усиленного интеллекта» при решении задач, нацеленных на предупреждение преступлений. Соответствующие программные средства могут применяться в целях криминалистического, оперативно-розыскного и экспертного предупреждения преступлений. В частности, они могут помочь выявить причины и условия, способствующие совершению высокотехнологичных преступлений, выделить потенциальные криминогенные объекты, прогнозировать отдельные аспекты готовящихся преступлений и т.п.

В качестве примера, для этих целей может использоваться исследовательская система honeypot. Эта система устанавливается на предполагаемый объект

преступного посягательства (объект изучения - сайт, сервер, виртуальную систему), к которому намеренно предоставляется относительно легкий несанкционированный доступ по информационной сети посредством заранее подготовленных уязвимостей в системе защиты. Такой подход позволяет получить криминалистически значимую информацию о готовящихся преступных посягательствах [35 - 37].

Специфика методологии современной криминалистики такова, что в нее легко включаются и адаптируются передовые методы, разрабатываемые другими науками. Считаем, что использование в криминалистике методов машинного обучения («усиленного интеллекта») имеет большие перспективы для выявления, расследования и предупреждения различных видов преступлений.

Библиографический список

1. Университеты на перепутье: Высшее образование в России [Текст] / Д. П. Платонова, Е. С. Абалмасова, С. К. Бекова и др.; под ред. Д. П. Платоновой, Я. И. Кузьминова, И. Д. Фрумина. - М.: Изд. дом Высшей школы экономики, 2019. - 319 с.
2. Батоев В.Б. Большие данные (big data)» и предиктивная аналитика в оперативно-разыскной деятельности: проблемы использования и пути решения // Вестник Волгоградской академии МВД России. – 2020. - № 1 (52). - С. 11-17.
3. Ушаков Р.М. Технология big data как вектор развития криминалистической техники: перспективы применения в контексте их правомерности // Уральский журнал правовых исследований. – 2020. - №2 (9). - С. 54-70.
4. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. - М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА•М), 2001. - 240 с.
5. Polyakov, V.V., Bespechniy, O.V., & Neymark, M.A. (2019). Artificial intelligence as an object of forensic study: perspectives from a border region. The role of transnational corporations in the globalization of the economy. *Advances in Social Science, Education and Humanities Research*, Vol. 364, Pp. 637-640
6. Вехов В.Б. Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. - 2019. - №2. - С. 630-640.
7. Ерахтина Е.А., Тирранен В.А. Преступления, совершаемые с использованием искусственного интеллекта: проблемы квалификации и расследования // Вестник Сибирского юридического института МВД России. – 2019. - №2. (35) – С. 36-41.
8. Поляков В.В. Начальные следственные ситуации расследования высокотехнологичных преступлений // Цифровые технологии в юриспруденции: генезис и перспективы [Электронный ресурс]: материалы I Международной межвузовской научно-практической конференции (28 февраля 2020 г., Москва) / НИУ МИЭТ, Краснояр. гос. аграр. ун-т, 2020. – С. 123-127.
9. Polyakov, V.V., Starodubtseva, M.A. (2019). Factors influencing motivation for terrorist activities being implemented with the use of information technologies in transboundary regions. The role of transnational corporations in the globalization of the economy. *Advances in Social Science, Education and Humanities Research*, Vol. 364, Pp. 188-191.
10. Белицкий В.Ю. Концепция криминалистической методики досудебного производства и судебного разбирательства мошенничеств: цели и задачи // Вестник Казанского юридического института МВД России. - 2020. - Т. 11, № 1 (39). - С. 63-68.
11. Россинская Е.Р. Проблемы современной криминалистики и направления ее развития // Эксперт - криминалист. - 2013. - №1. - С. 2-6.

12. Степаненко, Д.А., Бахтеева Д.В., Евстратова Ю.А. Цифровые технологии в современной криминологии // Всероссийский криминологический журнал. - 2020. - Т. 14, № 2. - С. 206–214.
13. Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной // Известия Томского политехнического университета. – 2007. – Т. 310, № 1. – С. 212-216.
14. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. ... канд. юрид. наук: 12.00.09. – Омск, 2008. – 247 с.
15. Поляков В.В. Основы формирования криминалистической методики расследования высокотехнологичных преступлений // Уголовное судопроизводство: правовое, криминалистическое и оперативно-розыскное обеспечение: монография / под ред. С.И. Давыдова. – Барнаул: Изд-во Алт. ун-та, 2019. – 214 с.
16. Хижняк Д.С. Криминалистическая классификация транснациональных преступлений // Юристъ-Правоведъ. - 2020. - № 2 (93). - С. 175-178.
17. Зуев С.В. Использование искусственного интеллекта для борьбы с преступностью в сети Интернет // Smart Law for Smart Industry : Сборник научных статей. Южно-Уральский государственный университет. Москва, 2020. С. 185-191.
18. Комаров И.М. Криминалистические операции и следственные ситуации в системе криминалистической характеристики расследования преступлений // Вестник Московского ун-та. Сер. 11. Право. - 2014. - № 4. - с. 50-61.
19. Быстрыков Е.Н., Усанов И.В. Криминалистическая характеристика преступления: происхождение, современное состояние, перспективы развития // Вестник Саратовской государственной юридической академии. - 2018. - № 6 (125) - С. 163-168.
20. Бахтеев Д.В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Сибирские уголовно-процессуальные и криминалистические чтения. - 2020. - № 2 (28). - С. 32-43.
21. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. - Томск: Изд-во Томского ун-та, 1985. - 333 с.
22. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2010. - №1 (21). - С. 46 - 50.
23. Драпкин Л.Я. Основы теории следственных ситуаций. - Свердловск: Изд-во Урал. ун-та, 1987. - 164 с.
24. Волчецкая Т.С. Криминалистическая ситуалогия: монография. / Под ред. проф. Н.П. Яблокова. - Москва; Калинингр. ун-т. - Калининград, 1997. – 248.
25. Зорин Г.А. Теоретические основы криминалистики. - Минск: Амалфея, 2000. - 416 с.
26. Видонов Л.Г. Криминалистические характеристики убийств и системы типовых версий о лицах, совершивших убийство без очевидцев. – Горький, 1978. - 121 с.
27. Густов Г.А. Программно-целевой метод организации раскрытия убийств. - СПб.: Институт повышения квалификации прокурорско-следственных работников прокуратуры РФ, 1993. - 121 с.
28. Лузгин И.М. Моделирование при расследовании преступлений. – Москва, 1981. - 152 с.
29. Розыходжаева Г.А., Розыходжаева Д.А. Особенности формирования обучающей выборки и обучения нейронной сети с неполными входными данными

при решении частных медицинских задач // Научное обозрение. Биологические науки. - 2017. - № 5. - С. 28-32.

30. Кафтанников И.Л., Парасич А.В. Проблемы формирования обучающей выборки в задачах машинного обучения // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. - 2016. - № 3. - С. 15-24.

31. Бертовский, Л.В. Цифровое судопроизводство: проблемы становления проблемы применения уголовного и уголовно-процессуального законодательства // Сборник материалов международной научно-практической конференции. Симферополь: Изд-во: «Ариал». - С. 173-178.

32. Власова С.В. К вопросу о приспособлении уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. - 2018. - № 1. - С. 9-18.

33. Бахтеев Д.В. Риски и этико-правовые модели использования систем искусственного интеллекта // Юридические исследования. – 2019. – № 11. – С. 1 - 11.

34. Еременко Ю.И., Шаталов А.А. Иммунный алгоритм мультиклональной селекции в решении задач идентификации почерка // Научные ведомости. - 2013. - № 22. - С. 218-224.

35. Craig V. Honeypot technologies and their applicability as a strategic internal countermeasure // International Journal of Information and Computer Security. 2011. - Vol. 1. - Issue 4. pp. 430-436.

36. Chuvakin A. Honeynets: High Value Security Data: Analysis of real attacks launched at a honeypot // Network Security. - 2003. - Vol.1. - Issue 8. - pp. 11–15.

37. Поляков В.В. Система honeypot как инструмент сбора информации для противодействия киберпреступности // Библиотека криминалиста : научный журнал. - 2017. - №1 (30). - С. 250-254.

APPLICATION OF MACHINE LEARNING METHODS IN FORENSIC RESEARCH ON THE EXAMPLE OF COUNTERING HIGH-TECH CRIME

Polyakov V.V.¹, Milic I.²

*¹Altai State University, Barnaul
e-mail: agupolyakov@gmail.com*

*²Faculty of Law, State University in Novi Sad, Republic of Serbia, Novi Sad
e-mail: i.milic@pf.uns.ac.rs*

Abstract. From a forensic point of view, the prospects for the use of machine learning and "enhanced intelligence" methods in countering high-tech crime have been investigated. For this, the features of modern crime that implement machine learning methods are analyzed, in particular, the emergence of new types and varieties of crimes in the field of computer information related to the use of machine learning methods is noted. The revealed patterns and features are proposed to be generalized and reflected in the corresponding criminalistic characteristics of crimes, as well as in the formation of typical criminal situations. The necessity of developing a new methodology for investigating crimes based on the use of machine learning methods and systems using algorithms of "enhanced intelligence" is substantiated. On the basis of such a methodology, the development of general forensic technical, tactical and methodological approaches to the investigation of crimes should be carried out. It is noted that expert practice can become one of the first applied forms of implementation of these technologies. Particularly promising is the use of machine learning methods and systems of "enhanced intelligence"

in solving problems aimed at preventing crimes, in particular, through the combined use of honeypots in research systems.

Keywords: machine learning, machine augmented intelligenc, high tech crime, forensic methodology