3. Залоило М. В., Власова Н. В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

4. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10. С. 35–37.

5. Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт // Научный вестник Омской академии МВД России. 2022. № 2. С. 101–105.

6. Мартьянов Н. Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. 2020. № 1. С. 175–177.

7. Статистика и аналитика // Официальный сайт МВД России. URL: https://мвд.рф (дата обращения: 06.09.2024).

8. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Сер.: Философские науки. 2021. № 1. С. 95–101.

9. Чуманов А. С. Проблемы противодействия незаконному обороту наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей // Киберпреступность: риски и угрозы. материалы Всерос. студ. круглого науч.-практ. стола с междунар. участием (г. Санкт-Петербург, 11 февраля 2021 г.). СПб. Астерион, 2021. С. 96–99.

Э. М. Гильманов,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирясова,
А. М. Бабаева,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК ДЛЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ЦИФРОВОЙ СФЕРЕ

Аннотация. В связи с цифровым развитием общества криминалистика тоже должна идти в ногу со временем и применять более современные инструменты и методики как для разработки, так и применения научных достижений во имя предотвращения нетривиальных преступлений, доселе невиданных.

Ключевые слова: искусственный интеллект, криминалистика, методы, преступление, цифровизация, киберпреступность, расследование

THE USE OF FORENSIC TECHNIQUES TO SOLVE CRIMES IN THE DIGITAL SPHERE

Abstract. Due to the trends in the development of society as a whole, criminology must keep up and apply more and more modern tools and techniques both

for the development and application of scientific achievements in the name of preventing non-trivial crimes hitherto unseen.

Keywords: artificial intelligence, criminology, methods, crime, digitalization, cybercrime, investigation

Введение. В соответствии с современными положениями российского законодательства о развитии искусственного интеллекта, это технология, позволяющая использовать мощности компьютерного устройства для анализа большого объема данных. И это, в силу его природы, превосходит скорость и качество работы, обусловленные отсутствием эмоций (человеческого фактора).

Перспектива синтеза искусственного интеллекта с работой органов предварительного следствия и разработкой новых методик представляется весьма успешной в силу титанических размеров баз данных, применяемых в ходе уголовного судопроизводства. Ведь, как известно, разнообразие способов совершения преступлений в цифровой сфере оставляет за собой и обуславливает возникновение цифровых следов [2. С. 130].

Основная часть. Как и у каждой группы преступлений, у киберпреступлений есть своя специфика. Ей являются многочисленные и разноплановые инструменты, используемые при их осуществлении. В этой связи уникальная правовая природа киберпреступлений определяет и особенности криминалистических методов по противодействию им [1. С. 170–171].

С одной стороны, криминалистические методы борьбы имеют свои подходы к толкованию киберпреступлений: большой объем информационных данных, потенциально обладающий признаками противообщественной направленности. Стоит отметить, что из всех настолько проработанная возможность совершения деяния при помощи компьютерных технологий обозначена только при мошенничестве [3. С. 36].

Так называемая компьютерная криминалистика, исходя из названия, предполагает использование в ходе расследования навыков по использованию цифровых и технологических достижений науки. Это будет способствовать разработке новых методов по сбору, анализу, сохранению и регистрации доказательств. Например, после получения результатов судебной экспертизы, следователи по борьбе с киберпреступностью связываются с компаниями, обеспечивающими подключение к информационно-телекоммуникационным сетям. Это происходит с целью выяснения, какие ресурсы или протоколы подключения использовались для совершения преступления [4. С. 30–31; 5. С. 650–668].

Еще не до конца изученными являются возможности искусственного интеллекта к самообучению: его пределы, скоростные лимиты, количество используемого трафика (данный вопрос создает дополнительный мотив к призыву компаний, обеспечивающих соединение искусственного интеллекта с информационно-телекоммуникационной сетью «Интернет» к сотрудничеству с органами уголовного розыска), что напрямую коррелирует с потенциальными возможностями методологии и инструментария криминалистики по отношению к расследованию киберпреступлений. Многими авторами исследуются вопросы принципов технологии искусственного интеллекта для успешного и эффективного его применения [6], что можно также весьма положительно оценить.

Заключение. Подводя итог, основополагающим отличием киберпреступлений является применение компьютеров в качестве «орудия» преступления. Соответственно, и методы криминалистической борьбы и противодействие им должны быть обеспечены новейшими достижениями компьютерной техники.

В частности, самым базовым применением искусственного интеллекта в борьбе с киберпреступлениями может послужить в качестве инструмента более качественный анализ данных по определенной категории преступлений (например, преступлений против половой свободы и половой неприкосновенности или преступления против экономики), включая запись камер видеонаблюдения, точные координаты места совершения преступления и т. д. Однако это упирается в нарушение конституционных прав и свобод человека и гражданина в плане сбора и применения личных данных преступника.

Список литературы

1. Болтенкова Ю. В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации // Поколение будущего: Взгляд молодых ученых – 2022: сборник научных статей 11-й Международной молодежной научной конференции, Курск, 10–11 ноября 2022 года. Том 2. – Курск: Юго-Западный государственный университет, 2022. – С 170–174. – EDN YZQBVM.

2. Климова Я. А . Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. №4 (55). URL: https://cyberleninka.ru/article/n/tsifrovaya-kriminalistika-perspektivy-razvitiya

3. Сарычев А. В., Архипцев И. Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий // ППД. 2020. № 1. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-raskrytiya-i-rassledovaniya-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionnyh-tehnologiy

4. Шевченко Е. С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3. С. 29–32. EDN SHOSCZ.

5. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности / Е. А. Русскевич // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. EDN FISEET.

6. Харитонова Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 1(2). С. 337–358. EDN: dxnwhv