Подходы борьбы с преступностью с использованием современных технологий в уголовном праве

Approaches to combating crime using modern technology in criminal law

DOI: 10.12737/2500-333X-2026-11-2-142-149

Коротченков Д.А.
Канд. юрид. наук, доцент кафедры уголовно-правовых дисциплин, Дальневосточный филиал ФГБОУВО «Российский государственный университет правосудия имени В.М. Лебедева», г. Хабаровск
e-mail: korotchenkov.d@mail.ru

Korotchenkov D.A.
Candidate of Law, Associate Professor, Department of Criminal Law, Far Eastern Branch of the V.M. Lebedev Russian State University of Justice, Khabarovsk
e-mail: korotchenkov.d@mail.ru

Пак З.А.
Студент 2 курса, Дальневосточный филиал ФГБОУВО «Российский государственный университет правосудия имени В.М. Лебедева», г. Хабаровск
e-mail: zlataslava.pak@mail.ru

Pak Z.A.
2nd year student, Far Eastern Branch of the V.M. Lebedev Russian State University of Justice, Khabarovsk
e-mail: zlataslava.pak@mail.ru

Аннотация
В данной научной статье рассматриваются концептуальные подходы к противодействию преступности непосредственно в условиях цифровой трансформации, в том числе проводится анализ процесса интеграции передовых технологий в теорию, а также практику уголовного права. Исследуется потенциал использования аналитики больших данных, а также различных инструментов прогностического моделирования для того, чтобы выявить горячие точки криминальной активности, в том числе превенции правонарушений. Уделяется внимание внедрению систем искусственного интеллекта в непосредственно следственную деятельность, которая включает в себя интеллектуальный анализ различных социальных сетей для деанонимизации преступных структур. Детально разбираются различные этические, а также правовые дилеммы, которые возникают при столкновении интересов общественной безопасности, а также конституционных прав граждан на конфиденциальность, в том числе защиту персональных данных. Рассматриваются перспективы международного сотрудничества, а также создания единых стратегий кибербезопасности.
Ключевые слова: уголовное право, современные технологии, большие данные, квалификация преступлений, цифровая трансформация, искусственный интеллект.

Abstract
This scientific article examines conceptual approaches to combating crime directly in the context of digital transformation, including an analysis of the process of integrating advanced technologies into the theory and practice of criminal law. The potential of using big data analytics, as well as various predictive modeling tools, is being explored in order to identify hot spots of criminal activity, including crime prevention. Attention is being paid to the implementation of artificial intelligence systems in direct investigative activities, which include the intelligent analysis of various social networks to de-anonymize criminal structures. Various ethical as well as legal dilemmas that arise when the interests of public safety collide, as well as the constitutional rights of citizens to privacy, including the protection of personal data, are examined in detail. The prospects of international cooperation, as well as the creation of unified cybersecurity strategies, are being considered.
Keywords: criminal law, modern technologies, big data, crime classification, digital transformation, artificial intelligence.

В современных реалиях стремительная трансформация общественных отношений, которая, в частности, вызвана глобальной цифровизацией, привела непосредственно к качественному, а также структурному изменению характера преступности. Устоявшиеся криминальные проявления эволюционируют, в связи с чем приобретают высокотехнологичный, анонимный, а также трансграничный характер. Правоохранительные органы всё чаще сталкиваются с беспрецедентными вызовами, которые начинаются кибертерроризмом, а заканчиваются использованием алгоритмов глубокого обучения непосредственно в целях мошенничества, а также эксплуатации людей. В таких условиях классические методы предупреждения, а также расследования преступлений, которые были образованы в эпоху аналогового права, демонстрируют значительное снижение эффективности, по причине того, что они не успевают за изменениями технологического ландшафта. Следовательно, кризис традиционных механизмов уголовно-правового воздействия вызывает острую необходимость концептуального пересмотра подходов непосредственно к обеспечению общественной безопасности населения, а также поиску инновационных решений, которые бы были способны обеспечить полную защиту прав личности, общества, а также государства в целом. Центральное место непосредственно в юридической дискуссии занимает вопрос интеграции различных современных технологий в систему уголовного права, а также правоприменительную практику. Но при этом, внедрение таких инструментов в сферу уголовной юстиции не заканчивается лишь техническими аспектами, так как оно порождает ещё очень серьёзные правовые, а также этические дилеммы. К ним относятся вопросы, которые связаны с допустимостью, а также достоверностью цифровых доказательств, необходимость нормативного закрепления уже новых процессуальных действий, а также определённый риск нарушения базисных принципов уголовного права. Результативная борьба с преступностью непосредственно в цифровую эпоху требует создания гибкой правовой базы, которая бы давала возможность использовать потенциал научно-технического прогресса.

В результате достаточно быстрой цифровизации общественных отношений уголовно-правовая доктрина, а также непосредственно криминологическая практика сталкивается с необходимостью перехода к использованию технологий больших данных. Как отмечает С.В. Рындина: «Технологии больших данных обеспечивают возможность обрабатывать массивы данных, хранящиеся распределённо из-за их масштабов; работать с потоковыми данными, которые образуются в информационных системах с большой скоростью в режиме реального времени; работать со структурированными и плохо структурированными данными параллельно в разных аспектах» [1, с. 8]. В сфере борьбы с преступностью применение аналитики больших данных даёт возможность обрабатывать очень большой объём неструктурированной информации, которая поступает из самых различных источников. Стоит отметить, что главная ценность данных технологий в уголовно-правовом аспекте заключается в том, что появляется возможность выявить скрытые корреляции, а также паттерны

криминального поведения, которые невозможно заметить методами традиционной экстраполяции. Всё вышеперечисленное создаёт базис для перехода к парадигме умного правопорядка, в котором главнейшим инструментом становится анализ всей информации для того, чтобы обеспечить общественную безопасность граждан.

Основным перспективным вектором интеграции современных технологий в деятельность непосредственно органов уголовной юстиции выступает прогностическая аналитика. Он основывается на использовании сложных алгоритмов машинного обучения, а также нейронных сетей для того, чтобы оценить вероятность совершения различных преступных деяний в будущем. Прогностическая аналитика, в отличие от реактивной модели правосудия, которая ориентируется на расследование уже совершённых преступлений, реализовывает превентивную функцию уголовного права, в которой оказывает воздействие на причины, а также условия преступности в режиме реального времени. Методологическая база данной аналитики основывается на интеграции трёх самых основных групп данных. Первой группой является ретроспективная информация об уже совершённых преступлениях, т.е. сюда относятся время, способ, а также специфика объекта посягательства. Далее следуют социально-экономические индикаторы, к примеру, такие как уровень безработицы, миграционные потоки, а также непосредственно показатели материального благосостояния в определённых участках. В-третьих, в обязательном порядке учитывается информация о демографических характеристиках населения, а также различных инфраструктурных особенностях конкретных районов. Обобщение этих данных позволяет аналитическим инструментам находить горячие точки преступности, то есть географические территории с самой высокой концентрацией риска криминогенной активности. Распознавание данных территорий даёт возможность правоохранительным органам осуществлять рациональное распределение конкретных ограниченных ресурсов.

В структуре цифрового общества непосредственно социальные сети преобразовались из обычных средств коммуникации между людьми в глобальные хранилища различных цифровых следов, которые содержат в себе крайне большой объём криминологически значимой информации. Во время использования органами уголовной юстиции технологий анализа социальных медиа перед ними открываются новые возможности для идентификации латентных угроз, а также деструктивных социальных связей. Анализ больших данных социальных сетей даёт возможность автоматизировать непосредственно процесс извлечения знаний о взаимодействиях между конкретными индивидами, при этом выявлять скрытые закономерности, которые остаются невидимыми при фрагментарном изучении определённых профилей. Непосредственно главнейшим инструментом в этом аспекте является анализ социальных графов, который даёт возможность визуализировать, а также математически обсчитать структуру криминальных сообществ. С помощью алгоритмов выявления сообществ, а также определения центральных узлов правоохранительные органы могут распознать формальных лидеров преступных группировок, а также, в частности, лиц, которые напрямую связаны с обеспечением коммуникации между отдельными ячейками. Стоит отметить, что всё это очень важно для борьбы с децентрализованными террористическим сетями, в том числе и наркосиндикатами, в которых традиционная иерархия обычно размыта. Наравне с этим, анализ метаданных, а также лингвистический анализ контента даёт возможность непосредственно фиксировать процессы радикализации отдельных пользователей или же групп на самых начальных стадиях, а также выявлять подготовку к совершению преступлений экстремисткой направленности до того момента, когда умысел перейдёт в стадию приготовления или покушения. Если рассматривать с точки зрения уголовно-правовой доктрины, то использование аналитики социальных сетей заметно увеличивает доказательственную базу, вследствие чего она позволяет квалифицировать деяния в качестве совершённых в составе организованной группы, а также преступного сообщества на основе объективных данных. Превентивный потенциал данных технологий даёт возможность реализовывать стратегии более раннего вмешательства, то есть правоохранительные органы могут осуществлять непосредственно адресное

профилактическое воздействие на лиц, которые вовлечены в деструктивные онлайн-сообщества. Но при этом внедрение таких методов глубокого анализа социальных медиа требует очень тщательной правовой регламентации для того, чтоб обеспечить баланс между интересами общественной безопасности, а также конституционными гарантиями прав граждан.

Интеграция систем искусственного интеллекта непосредственно в деятельность органов предварительного расследования обозначает переход к более высокотехнологической модели доказывания, в которой скорость, а также точность обработки визуальной информации становится решающим фактором, так как данная система способна оперировать очень большими массивами данных в реальном времени. Наиболее востребованными технологиями в современной криминалистической практике являются непосредственно системы автоматического распознания лиц. Они базируются на нейронных сетях, которые осуществляют декомпозицию человеческого лица на особенные биометрические параметры, то есть создаётся цифровой отпечаток, который в дальнейшем сопоставляется с базами данных оперативных учётов, паспортных столов, а также записями из каких-либо открытых источников. Использование системы автоматического распознания лиц в рамках систем «Безопасный город» как отмечает Д.В. Кофман: «Позволяет значительно ускорить процесс раскрытия преступлений, сократить количество ошибок, связанных с человеческим фактором и улучшить качество работы криминалистов» [2, с.117]. В аспекте уголовно-правовой доктрины, результаты работы данных систем распознания лиц ставят вопрос об их непосредственном доказательственном значении. Высокая степень точности современных алгоритмов даёт возможность использовать такие данные в качестве весомого косвенного доказательства, но также это требует очень строгого соблюдения процессуальной формы, а также возможности проведения независимой технической экспертизы алгоритма на случай оспаривания результатов. Также стоит отметить, что внедрение вышеуказанных систем сталкивается с довольно серьёзными правовыми, а также этическими барьерами. Основным из них является конфликт между интересами общественной безопасности, а также конституционным правом граждан на неприкосновенность частной жизни, а также защиту персональных данных. Риск формирования цифрового паноптикума, в котором абсолютно каждое перемещение гражданина фиксируется без его согласия, вызывает в обществе оправданные опасения. Наравне с этим, исследования показывают, что точность распознания может изменяться в зависимости от расовой принадлежности, пола, а также возраста индивида, поэтому создаётся риск ложных обвинений, а также прямого нарушения принципа презумпции невиновности. Следовательно, применение таких технологий в уголовном праве крайне нуждается в детальной законодательной регламентации, так как необходимы чёткие критерии допустимости использования технологий распознавания лиц, установление сроков хранения биометрических данных, а также непосредственно определения круга лиц, которые будут иметь доступ к ним. Правовое регулирование в обязательном порядке должно исключать любую возможность нецелевого использования технологий, а также гарантировать, что внедрение искусственного интеллекта будет служить только целям правосудия, а также защиты граждан от любых преступных посягательств.

Развитие уголовной юстиции характеризуется беспрецедентным, а также очень стремительным ростом преступности непосредственно в цифровой среде, вследствие чего, перед правоохранительными органами возникают новые вызовы, которые не имеют аналогов в прошлом. Как констатируют эксперты: «За последние пять лет количество преступлений, совершенных в сфере информационно-телекоммуникационных технологий, возросло более чем в шесть раз» [3]. В аспекте уголовного права данная динамика означает непосредственно качественное усложнение всего процесса доказывания главных элементов состава преступления, поэтому требуется внедрение систем искусственного интеллекта для того, чтобы автоматизировать аналитические процедуры. Со стороны уголовного права автоматизация расследований на основе искусственного интеллекта очень важна для того, чтобы правильно юридически квалифицировать различные деяния. В преступлениях, которые

совершаются в цифровой среде, установление объективной стороны в большинстве случаев затруднено из-за множественности транзакций, распределённости сетевых атак, а также использование анонимайзеров. Такие системы искусственного интеллекта дают возможность автоматизировать весь процесс сопоставления непосредственно фактических действий субъекта с диспозициями статей Особенной части Уголовного кодекса Российской Федерации. Наравне с этим, появляется возможность выявлять устойчивые связи между цифровыми следами, а также конкретными преступными последствиями. Всё вышеперечисленное обеспечивает соблюдение принципа законности, но при этом способствует исключению произвольного толкования признаков состава преступления при обработке массивов данных.

Большое значение автоматизация имеет для установления субъективной стороны преступления, то есть доказывание вины, а также прямого умысла. Интеллектуальный анализ переписок, а также сетевого поведения конкретных лиц, который проводится специальными алгоритмами, даёт возможность выявить признаки предварительного сговора, в том числе и подготовку к совершению преступления, которые в ручном режиме обработки информации чаще всего остаются латентными. В делах о соучастии искусственный интеллект становится незаменимым инструментом для того, чтобы доказывать признаки организованной группы, в том числе преступного сообщества, который непосредственно выстраивает иерархические графы связей, а также распределение ролей между конкретными участниками на основе их цифровой активности.

Ещё одно глубокое уголовно-правовое значение имеет автоматизация самого процесса формирования обвинительных документов, так как правильное описание способа совершения преступления, а также мотивация субъекта непосредственно в постановлениях, в том числе и обвинительных заключениях, выступает гарантией против судебных ошибок. С помощью систем поддержки принятия решений следователь с очень высокой точностью может сформулировать фабулу обвинения, которая будет соответствовать актуальным разъяснениям Пленума Верховного суда Российской Федерации, вследствие чего, повышается обоснованность уголовного преследования.

Стоит отметить, что внедрение автоматизации ставит непосредственно перед наукой уголовного права базисный вопрос о соблюдении принципа вины. По причине того, что использование чёрных ящиков алгоритмов ни в коем случае не должно подменять собой личное убеждение следователя, а также судьи о виновности конкретного лица. В уголовно-правовом аспекте не допускается делегирование полномочий по окончательной правовой оценке деяния лица искусственному интеллекту. Вследствие чего, интеллектуальная автоматизация должна рассматриваться в роли механизма обеспечения чистоты, а также точности уголовно-правовой квалификации.

Ввиду процесса цифровизации абсолютно всех сфер общественной жизни информационное пространство преобразовалось в самостоятельную область правового регулирования, а также охраны. Уголовное право выступает крайне жёстким инструментом государственного регулирования, которое на постоянной основе сталкивается с необходимостью приспособления к новым способам посягательств, в которых непосредственно информация является объектом преступления.

Если рассматривать с позиции уголовного права, то защита информации выступает комплексным правовым институтом, который обеспечивает полную неприкосновенность общественных отношений. Как отмечают эксперты по цифровой криминалистике: «В 2025 году количество атак программ-вымогателей выросло на 15% по сравнению с предыдущим годом» [4]. Рост числа кибератак ставит перед всей правовой наукой задачу непосредственно точной идентификации признаков состава преступления в действиях, которые нарушают устоявшиеся режимы информационной безопасности. Следует отметить, что значимость кибербезопасности конкретно в уголовно-правовом аспекте увеличивается прямо пропорционально сложности технологий, которые используют преступники, то есть, к примеру, распределённые атаки, а также методы социальной инженерии. Самым главным

элементом уголовно-правовой квалификации киберпреступлений выступает категория неправомерности доступа. В данном случае различные технические меры защиты информации приобретают юридическое значение, так как их непосредственное преодоление может служить объективным признаком наличия преступного умысла лица, а также противоправности его действий. В том случае если информация не защищена специальными мерами, то доказывание состава преступления может быть сильно усложнено, потому что непосредственно взлом или же обход защиты демонстрирует общественную опасность деяния, следовательно, квалифицирует его как нарушение установленного правового режима. Также актуальность приобретает уголовно-правовая охрана критической информации инфраструктуры. Защита информации здесь рассматривается в качестве непосредственного вопроса национальной безопасности, а за нарушение определённых правил эксплуатации систем или же незаконное воздействие на них влечёт повышенную ответственность. Следовательно, государственная уголовная политика в обязательном порядке должна опираться на тесное взаимодействие правоохранительных органов с частным сектором, так как большая часть информационных систем, а также банков данных, находится в непосредственном ведении частных корпораций. Межсекторальное сотрудничество правоохранительных органов с частными компаниями непосредственно в аспекте разработки стратегий для защиты данных является очень важным нюансом для доказывания. С помощью оперативной передачи телеметрических данных даёт возможность следствию установить объективную сторону преступления. Если рассматривать с точки зрения уголовного права, то данное взаимодействие содействует реализации принципа неотвратимости наказания, потому что позволяет перевести уголовную политику в предотвращение каких-либо преступных последствий.

Одной из самых сложных проблем современной доктрины непосредственно уголовного права выступает преодоление диссонанса между национальным характером уголовной юрисдикции, а также транснациональной природой самой преступности в цифровой среде. Киберпреступность сама по себе не имеет государственных границ, поэтому эффективность реализации принципа неотвратимости уголовной ответственности находится в зависимости от качества международного сотрудничества, а также способности государств гармонизировать непосредственно свои правовые системы для того, чтобы совместно противодействовать всем глобальным киберугрозам. Данное сотрудничество является необходимым инструментом для того, чтобы разрешать коллизии юрисдикции, а также выявлять места совершения преступлений. Базисные институты международного права непосредственно в аспекте киберпреступлений требуют значительной модернизации. Стоит отметить, что уголовно-правовое значение такого сотрудничества состоит в том, чтобы узаконить различные цифровые доказательства, которые находятся на иностранных серверах. Без вышеперечисленных механизмов межгосударственного взаимодействия очень многие составы, которые предусмотрены непосредственно гл. 28 Уголовного кодекса Российской Федерации, рискуют остаться декларативными из-за того, что невозможно идентифицировать конкретный субъект, который находится вне пределов национальной юрисдикции.

Главнейшим этапом в данном направлении выступает гармонизация национальных уголовных законодательств, так как существуют правовые зоны с очень мягким или же вовсе отсутствующим регулированием киберпреступлений, которые подрывают глобальные усилия по обеспечению информационной безопасности. Международное сотрудничество должно взят вектор на выработку непосредственно единых дефиниций составов преступлений, а это, в свою очередь, даст возможность избежать отказов в выдаче преступников ввиду отсутствия признака двойной криминализации. Создание, а также непосредственное использование совместных баз данных правоохранительных органов получает процессуальное значение, так как обмен всей необходимой информацией о различных новых способах совершения преступлений, а также оперативная передача данных о кибератаках дают возможность вовремя пресекать преступную деятельность на стадии приготовления или же покушения.

Международное сотрудничество содействует выработке единых стандартов ответственности для различных транснациональных преступных сообществ. Интеграция правовых систем с помощью создания совместных следственных групп, а также механизмов реального времени для того, чтобы фиксировать цифровые следы позволяет рассматривать киберпреступность в качестве глобального вызова, который требует универсального уголовно-правового ответа. Следовательно, проблема суверенитета в цифровом пространстве должна решаться непосредственно через создание прозрачных протоколов взаимного доступа к криминалистически важной информации при обязательном соблюдении прав человека, а также норм международного права.

Важно отметить, что применение систем тотального видеонаблюдения непосредственно с функцией распознавания лиц, специальных алгоритмов предиктивной аналитики, а также методов глубокого анализа больших данных неминуемо вступает в конфликт с базисным правом граждан на неприкосновенность частной жизни. Непосредственно в уголовно-правовой доктрине право на конфиденциальность выступает неотъемлемым условием свободы личности, поэтому любое вмешательство в данную сферу со стороны государства должно быть в обязательном порядке обоснованным. Как отмечает Л.В. Чеснокова: «В последние десятилетия в связи с бурным развитием информационно-коммуникационных технологий... Появились риски утраты контроля доступа к личной информации. Это вызывает опасения по аналогии с цифровым паноптикумом» [5, с. 137].

Основной проблемой здесь является допустимость, а также легитимность всех доказательств, которые получены с помощью скрытых алгоритмических систем. В том случае, если правоохранительные органы используют специальные инструменты массового сбора необходимых данных непосредственно без надлежащего судебного контроля, то это подрывает базис справедливого правосудия. Право на защиту данных преобразовывается в элемент цифрового достоинства личности, а в случае нарушения оно должно влечь за собой определённые правовые последствия. Наравне с этим, алгоритмизация уголовного процесса порождает угрозу нарушения презумпции невиновности в том случае, когда искусственный интеллект отмечает человека в роли потенциального правонарушителя, в результате чего появляется риск предвзятого отношения непосредственно со стороны субъектов правоприменения, а такое недопустимо. Следовательно, для того, чтобы устранить данные риски необходимо разработать, а также закрепить на законодательном уровне определённые правовые рамки, которые будут регулировать использование инновационных технологий правоохранительными органами. Также необходимо внедрить механизмы прозрачности алгоритмов для того, чтобы сторона защиты имела возможность оспорить автоматизированное решение, которое стало основанием для ограничения прав конкретного гражданина. Законодательное регулирование должно чётко определять границы использования биометрических данных, в том числе информации из каких-либо социальных сетей, а также при этом исключать возможность их нецелевого использования.

Интеграция современных технологий непосредственно в систему борьбы с преступностью является объективной необходимостью для того, чтобы сохранить дееспособность института уголовного права в условиях цифрового преобразования. Все вышеперечисленные инструменты, то есть предиктивная аналитика, непосредственно системы распознавания лица, в том числе интеллектуальная автоматизация следственных процессов, обладают очень большим потенциалом для того, чтобы реализовывать принцип неотвратимости наказания, а также обеспечивать общественную безопасность всех граждан. Но при этом технологический прогресс не должен опережать развитие правовой мысли. Эффективность борьбы с преступностью находится в непосредственной зависимости от качества правовой регламентации всех инноваций, которые используются. В перспективе развитие подходов к борьбе с преступностью в обязательном порядке должно идти по пути совершенствования норм Особенной части Уголовного кодекса Российской Федерации, гармонизации международного законодательства, а также создания прозрачных протоколов работы с цифровыми данными. Следовательно, крайне необходимо формировать этико-

правовые стандарты применения новых технологий, что в обязательном порядке будет включать в себя механизмы верификации алгоритмов, а также защиты конфиденциальности всех граждан.

Литература

1. Рындина С.В. Технологии анализа больших данных (продвинутый уровень): управление и руководство данными, хранение и обработка данных [Электронный ресурс]: учебно-методическое пособие / С.В. Рындина. - Пенза: ПГУ, 2023. - 48 с. - URL: https://elib.pnzgu.ru/files/eb/OOXI6RKBwfNz.pdf
2. Кофман Д.В. Использование аппаратно-программного комплекса «Безопасный город» в целях выявления и раскрытия преступлений / Д. В. Кофман // Молодой ученый. – 2023. - № 38. – С.117-120. - URL: https://moluch.ru/archive/485/106114
3. Портал правовой статистики Генеральной прокуратуры Российской Федерации [Электронный ресурс] // URL: http://crimestat.ru/analytics (дата обращения: 26.04.2026).
4. Киберугрозы-2025: F6 назвала основные тренды вымогателей, утечек, фишинга [Электронный ресурс] // URL: https://companies.rbc.ru/news/PptyKOK1Ua/kiberugrozyi-2025-f6-nazvala-osnovnyie-trendyi-vyimogatelej-utechek-fishinga/ (дата обращения: 26.04.2026).
5. Чеснокова Л.В. Цифровая медиасреда и проблемы приватности / Л.В. Чеснокова // Вестник Гуманитарного университета. - 2025. - № 1. - С. 136–145. - URL: https://vestnik.gu-ural.ru/documents/articles/2025/1/gu-2025-1-chesnokova.pdf