УДК/UDC 343.974

Перспективы развития криминологии в киберпространстве

Исаева Мария Андреевна
студентка юридического факультета
Московский университет им. С. Ю. Витте
г. Москва, Россия
e-mail: masis2001@mail.ru

Кислый Олег Алексеевич
кандидат педагогических наук, доцент кафедры административно-правовых дисциплин и таможенного дела
Московский гуманитарно-экономический университет
г. Москва, Россия
e-mail: razboiniki@yandex.ru
SPIN-код: 4737-6134

Аннотация

Мир XXI в. испытывает на себе глобальные метаморфозы. Формирование общества, где главную роль играет информация, развитие современных технологий, создание искусственного интеллекта ставит новые вызовы перед человечеством. Правовую сферу как весьма значимую часть жизни общества также не обошли данные трансформации. Развитие цифровизации и создание искусственного интеллекта для гуманитарного знания, юридического образования, профессии юриста и в целом юриспруденции в действительности можно отнести к вызовам общества современности. В статье рассматриваются перспективы развития криминологии в киберпространстве. Исследуется такое явление, как цифровое профилирование. Отмечается, что стремительный темп развития киберпреступности опережает отклик правоприменителя на расследование правонарушений в данной области. В связи с этим особое значение приобретает исследование иностранного опыта и внедрение правоохранительными органами цифровых технологий в практику борьбы с киберпреступностью.

Ключевые слова: искусственный интеллект, цифровая экономика, меры противодействия, право, юридическая деятельность, цифровая криминология, современные технологии противодействия преступности, киберпреступления, кибербезопасность.

Development prospects of the criminology in cyberspace

Isayeva Mariya Andreyevna
student of the Faculty of Law
S. Yu. Witte Moscow State University
Moscow, Russia
e-mail: masis2001@mail.ru

Kislyy Oleg Alekseyevich
Candidate of Pedagogical Sciences, Lecturer of the Department of Administrative and Legal Disciplines and Customs Affairs
Moscow University of Humanities and Economics
Moscow, Russia
e-mail: razboiniki@yandex.ru
SPIN Code: 4737-6134

Abstract

World of the XXI century. is experiencing global metamorphoses. The formation of a society where information plays the main role, the development of modern technologies, the creation of artificial intelligence poses new challenges to humanity. The legal sphere, as a very significant part of the life of society, was also not spared by these transformations. The development of digitalization and the creation of artificial intelligence for humanitarian knowledge, legal education, the legal profession and, in general, jurisprudence can in fact be attributed to the challenges of modern society. The article discusses the prospects for the development of criminology in cyberspace. The phenomenon of digital profiling is being investigated. It is noted that the rapid pace of development of cybercrime is ahead of the response of the law enforcement officer to the investigation of offenses in this area. In this regard, the study of foreign experience and the introduction of digital technologies by law enforcement agencies into the practice of combating cybercrime is of particular importance.

Key words: artificial intelligence, digital economy, countermeasures, law, legal activity, digital criminology, modern technologies for combating crime, cybercrime, cybersecurity.

Становление экономики «цифры» — одно из приоритетных направлений большинства стран — экономических лидеров. В Российской Феде-

рации быстрое введение информационных технологий в экономическую сферу и жизнь социума является одной из национальных целей развития [1]. Именно эффективное использование новых цифровых технологий в ближайшем будущем определит международную конкурентоспособность как отдельных компаний, так и целых стран, формирующих инфраструктуру и правовую среду для цифровизации [2].

Конечно, сегодня растет в геометрической прогрессии количество, качество и многообразие взаимосвязей между организациями, гражданами, социально-экономическими институтами и системами, сопровождающееся динамичным «квантовым скачком» числа транзакций и объемов данных, приводящих к более комплексной и синхронизированной интеграции «всех со всеми». Такие положительные тенденции в сотрудничестве уже сейчас требуют от единиц общества новых навыков и компетенций, готовности использовать новые информационные средства в повседневной жизни.

Однако, чем «умнее» становятся устройства доступа, тем потенциально выше уровень уязвимости владельца. Распространение IT-технологий делает человека фактически «прозрачным» для любых заинтересованных лиц и структур, что, в свою очередь, порождает спрос на развитие технологий информационной безопасности и технологий киберпреступности. Обществу предстоит справиться с нарастающими опасениями негативных последствий цифровизации, среди которых выделяется рост масштабов компьютерной преступности, незащищенность прав человека в цифровом пространстве, угрозы сохранности цифровых пользовательских данных и пока еще низкий уровень доверия к цифровой среде.

Наравне с формированием и развитием экономики, медицины, образования, укреплением обороноспособности страны прогноз преступности, ее предупреждение и противодействие ей с применением передовых технологий также должны занять главенствующее место в задачах государства.

Юридическая информация и закон в целом имеют большую стоимость, будучи «ядром» защиты жизни и имущества людей; это «код», регулирующий общественную жизнь. Рынок электронных юридических услуг находится на сравнительно ранней, но очень важной стадии своего развития относительно разрушительного влияния искусственного интеллекта на монополию юристов. Искусственный интеллект будет играть все более важную роль в пяти областях юридической деятельности: поиске информации по обстоятельствам дела, поиске прецедентов, составлении документов, подготовке материалов дела и прогностической аналитике.

Бесценный вклад в изучение способностей и перспектив сегодняшних IT-технологий внесли В. С. Овчинский и Е. С. Ларина [3]. Они рассматривали машинный разум как «ноу-хау», которое преследует цели тройного назначения — гражданские, военные и криминальные [4]. Современная преступность характеризуется тем, что умеет взять и эксплуатировать в своих целях прогрессивные труды техники. Это объясняется некой «прозрачностью» академических достижений — масштабное применение открытого кода позволяет злоумышленникам без особых усилий заполучить доступ к последним исследованиям и разработкам лидирующих организаций.

Личность преступника и природа его преступных намерений всегда были и остаются одной из краеугольных проблем всех наук криминального профиля.

Преступность и преступное поведение — объект юридических и социологических исследований. Юриста интересует наряду с правотворчеством природа нарушения норм законодательства, особенно уголовного, общие и специфические причины или условия, способствующие воспроизводству и распространению преступности. Здесь на помощь приходит наука криминология. Для криминологии особенной ценностью является анализ механизма преступного посягательства, который представляет собой взаимосвязь объективных и субъективных факторов, детерминирующих совершение преступления.

То, как мыслит преступник, оказывается более искусным, в отличие от умственных, координационных и других действий органов правопорядка. В соответствии с официальными данными статистики Министерства внутренних дел Российской Федерации в первом квартале 2021 г. зафиксировано на 33,7% больше преступлений, чем год назад, в т. ч. с использованием информационно-телекоммуникационной сети «Интернет» — на 51,6% и при помощи средств мобильной связи — на 31,6% в IT-сфере. В январе–марте 2020 г. такие нарушения составили 19,9% от общего числа зарегистрированных преступлений, а за три месяца текущего года этот показатель вырос до 27,1% [5].

Благодаря анализу и познанию нынешней сверхтехнологичной преступности, можно обозначить такие методы и области применения преступниками «искусственного мозга»:

1. Фишинг («выуживание») — тип интернет-мошенничества, целью которого является приобретение допуска к секретной и конфиденциальной информации пользователя. Так, многочисленные рассылки корреспонденции и писем по электронной почте от якобы популярных марок и брендов содержат ссылки на мошеннические сайты, внешне похожие на настоящие. Это приводит к тому, что пользователи, переходя на указанную страницу в информационно-телекоммуникационной сети «Интрнет», вводят свои логины и пароли, а аферисты таким образом получают доступ к аккаунтам и банковским счетам своих жертв.
2. Использование управляемых искусственным интеллектом дронов в мошеннических целях (контрабанда запрещенных предметов и веществ, поставка различных вещей в места лишения свободы).
3. Хакерские атаки, распространение дезинформации, «фейков» [6].
4. Использование ботов — программ, которые, следуя конкретному алгоритму, выполняют какие-либо действия, например общаются с пользователями различных сайтов, чатов, социаль-

ных сетей и т. д. Так в 2017 г. боты небывало атаковали социальную сеть «ВКонтакте» — отправляли приглашения людям в личных сообщениях в печально популярные «группы и сообщества смерти». На сайте описываемой социальной сети с начала 2021 года было сгенерировано примерно три миллиона уведомлений с текстом, призывающим к совершению суицида [7].

«Маркерами» правонарушений, в которых использовались средства информатизации, являются значительный уровень анонимности и латентности, но в некоторых случаях (пример с ботами) почти исключается из преступной цепочки личность злоумышленника, что не может не вызывать чувство безнаказанности.

Решение проблем обеспечения безопасности альтернативным традиционным методам способом правоохранительной деятельности позволяет технология «Big data». Информационная методика «Big data» заключается в обработке информации огромных объемов для получения воспринимаемых человеком результатов в условиях непрерывного прироста этих данных (например, поведение человека в социальных сетях и т. д.). Данная технология обработки мегамассивов данных позволяет искать ценные закономерности, факты и другую информацию, имеющую значение для разных видов правоохранительной деятельности. Перспективы применения указанных технологий многообразны, например розыск лиц, скрывающихся от правоохранительных органов, путем мониторинга социальных сетей и систем видеофиксации.

В них нельзя не оставить «цифровые отпечатки», ведь они отражают персональные поведенческие особенности индивида. Чаты, блоги, форумы, социальные сети и т. д. включают исходную информацию о случившемся иного качества. Так, в киберпространстве в течение некоторого периода времени сохраняются «электронные маячки» взаимодействия человека с цифровой средой. Это и есть информационные следы преступления, а равно и поведенческие признаки индивида в среде IT-технологий. При расследовании компьютерных преступлений цифровая электроника выступает сегодня в роли носителя свойств составов право-

нарушений, отраженных в киберпространстве, а серверные устройства — в роли носителей преступных следов.

Это свидетельствует о том, что в арсенале субъектов расследования в эпоху цифровых технологий центром должны стать качественно иные средства изучения преступных посягательств в среде «цифры». В первую очередь речь идет о методах и способах, которые основаны на исследовании содержания колоссального объема информации, а также о привлечении специалистов и экспертов со специальными знаниями в области обработки цифровой криминологической информации.

Какое «лицо» у будущей криминологии? Существуют ли шансы ее дальнейшего развития?

Данные вопросы стали волновать ученых относительно недавно. Однако их актуальность поддерживается не столько сложившимися в науке условиями, касающимися обстоятельств совершений преступлений и закономерностей ее становления, сколько наличием прогнозов исследователей о будущем социума и цивилизации в целом. Трудно сказать о проектах стратегий дальнейшего развития науки криминологии, ведь нет «сильного» вектора тактики ее существования и, конечно же, критической оценки этих концепций. В настоящее время современное состояние криминологической теории серьезно обсуждается научной средой — самые опытные ученые-криминологи обращают внимание на отсутствие современной методологии криминологических исследований, отставание отечественной криминологической теории от зарубежных исследований. Высказывания о будущей криминологической мысли не могут не содержать анализ фундаментальных научных категорий современности, ведь даже общие особенности эволюции нынешней российской криминологии не вселяют научным работникам оптимизма, что дает возможность заявлять об ослабевании криминологических исследований, об их наукоподобности и простоте, терминологической несогласованности и раздробленности. А это лишь доля трудностей.

Цифровая («вычислительная») криминология давно уже стала теоретической реальностью, но лишь сегодня, главным образом в результа-

те появления качественно новых криминальных вызовов, она имеет все шансы быть востребованной в практике борьбы с преступностью, прежде всего с организованными ее формами.

Применение «машинного мозга», роботов, криминальной 3D-печати, биотехнологий должно привести к формированию и становлению ранее неизвестных технологий противозаконного поведения, ведь противоположная сторона технологической эволюции преступности в информационной среде — интенсивное осваивание ей новейших областей: робототехника, синтетическая биология, искусственный интеллект. Данные обстоятельства поднимают «уязвимость» криминологической безопасности на новый уровень. Если специалисты делают прогноз метаморфоз норм социума путем замены их присутствующими в киберпространстве виртуальными нормами, которые, в свою очередь, «дарят» человеку допустимость более свободно социализироваться с учетом своих скрываемых в обычном обществе нужд, то никак не наблюдать их криминогенного нюанса криминологам нереально.

Структурирование и моделирование цифрового портрета неустановленного преступника (Digital Profiling) становится возможным. Цифровое профилирование как способ расследования обладает особой ценностью, когда сложно сравнить отдельный цифровой прибор с конкретным пользователем (как образец, в случае если мы имеем одно коммуникационное устройство и несколько пользователей).

Согласно результатам использования растрового метода лица, подпадающие под категорию потенциального подозреваемого, подлежат последующей проверке и контролю на причастность к содеянному правонарушению. Проверка и контроль осуществляются при поддержке традиционных следственных и оперативно-розыскных средств и методов (опросов, допросов, электронного наблюдения, обысков и т. д.).

Преступное поведение, как правило, неповторимо и эпизодично. В нем четко можно рассмотреть логические закономерности между способами, орудиями совершения преступления и социально-психологическими отличительными чертами лица, которое совершило

общественно опасное деяние. Ведь орудия, средства преступления, способ его совершения злоумышленник выбирает, исходя из опыта жизни, социальных ролей в обществе, структурных характеристик личности (эмоциональные, волевые, интеллектуальные, нравственные и др. признаки). Профессиональные, преступные умения, отображающие социальные качества и роли лица, «включаются» в роли криминологического фактора посредством определенного влияния на них. При криминальных условиях, в преступных ситуациях индивид функционирует таким образом, каким приспособился действовать в подобных ситуациях ранее. Если мы говорим о серийном или рецидивном преступнике, то при соответствующем анализе и исследовании его поведения можно установить и сформировать уникальную модель действий.

Преступное поведение содействует выявлению и установлению повторяемости преступлений и характеризуется обширным диапазоном присущих ему явлений и процессов, но остаются три важнейших компонента: способ совершения преступления («modus operandi»), социальные показатели индивида (эмоционально-волевые признаки или психологические особенности) и почерк преступления (уникальные комбинации поведения).

Несмотря на то, что метод профайлинга благополучно применяется в Российской Федерации, в последнее время новых исследований в данной сфере практически не появляется, хотя проблема его использования при раскрытии и расследовании преступлений является актуальной.

Криминологи признают актуальными, востребованными сегодняшним состоянием науки возможности методологического многообразия с нестандартными методами, используемыми в качестве дополнения и добавления уже к существующим методикам, формирование количественной криминологии. Также выдвинуты теории о перспективах внедрения идей философской и психологической наук, которые до сих пор не включались в методологию криминологии, но целесообразны при решении криминологических задач. Многие думают, что вопрос личности преступника и без того всецело исследован криминологами. Однако, невзи-

рая на большое количество работ о личности злоумышленника, в криминологии пока в существенной мере превалирует механистичное, облегченное мнение о личности преступника при очевидном обезличивании, малом учете либо вообще пренебрежении отличительными чертами личности преступника в правоприменительной работе. Вместе с тем природа человека содержит склонность к преступлениям, а то, осуществит или не осуществит конкретный человек правонарушение, зависит прежде всего от случайного стечения факторов и обстоятельств. А потому вновь актуализировался вопрос о том, чтобы сделать личность «ядром» криминологической и уголовно-правовой проблематики [8].

В настоящий период цифровое профилирование, которое производно от традиционного профилирования в общепризнанном представлении, с успехом применяется в европейских странах [9]. Данный тип профилирования предполагает взаимосвязь сложных технических действий обработки и анализа информации криминологического интереса, база которых строится на логико-математических методах. Подобная отличительная черта «дает разрешение» использовать рассматриваемый метод в расследовании в ситуациях интеграции персональных многофункциональных устройств в IT-сфере.

В целом профилирование «цифры» значимо при расследовании серийных преступлений, в частности в противоправных деяниях, инструментом, способом или местом совершения которых являются компьютеры, цифровые устройства и цифровая среда, т. е. в киберпреступлениях. Процедура цифрового профилирования предполагает собой цепочку поочередных операций:

1. Определение «начальной миссии»: поиск необходимой информации в соответствии с конкретным случаем.
2. Сбор, анализ сведений, включающих нужные данные.
3. Отбор подходящей информации и получение указателей для каждой из рассматриваемых сфер познания.
4. Сопоставление указанных данных для нахождения противоречий или сходства.

5. Определение критериев, сравнение и формирование «цифрового профиля».
6. Анализ полученного «цифрового профиля» в сопоставлении с «начальной миссией».

Метод научного познания «точная экстраполяция» получил максимальное продвижение в криминологии. Он дает возможность численно дать оценку познания об объектах, явлениях, действиях, процессах при конкретных обстоятельствах и в дальнейшем трансформировать на другие. Установленный способ основан на наблюдении за существующими сегодня тенденциями и закономерностями формирования преступности.

Диагностирование профиля преступника и последующее определение полученного профиля — цель многомерной экстраполяции модификации действий. Необходимо отметить, что в отечественной доктрине теоретические принципы основываются на академических утверждениях криминалистики, криминологии, информатики и др. Диагностика, к сожалению, пока не дает определение таким понятиям, как «идентификация», «определение групповой принадлежности и диагностики», «диагностика и прогнозирование», «диагностика и аналитический поиск».

Например, социальный аспект в поведении хакера и его почерк в цифровом мире являются «товарным знаком» и отражают потребность правонарушителя, совершая преступления, «выразить себя», что демонстрирует его индивидуальность, личность. Очевидным становится проявление личных отличительных криминальных черт, качеств, наклонностей при похищении данных и написании разрушающего программного обеспечения для несанкционированного вторжения в посторонние системы, удаления или изменения значимых сведений. Мотивы, способы и цели при совершении киберпреступлений также разнообразны. В контенте технологий «цифры» язык программирования делается более сложным и динамичным, в особенности в сетевых виртуальных сферах.

Так, более сложным типом умственной деятельности в системе криминологический исследований становится использование методов цифрового профилирования в расследовании, в т. ч. в киберпространстве.

Проведение такого рода исследований, по мнению иностранных специалистов, считается сложной задачей в сравнении с классическими способами расследования. Основными факторами, порождающими затруднения, признаются:

1) расхождение и недостаточность документирования;
2) трудности интеграции природы человека и технологий;
3) проявляющееся подозрение в правдивости итогов классического криминологического профилирования и психологических изучений.

Итак, способ цифрового профилирования можно воспринимать как специальный прием, применяемый в расследовании, уникальность которого состоит в исследовании и рассмотрении с помощью электронно-вычислительной машины больших объемов данных, синхронный анализ которых не возможен субъектом расследования. Математические методы моделируют алгоритм определения правонарушителя по предварительно составляемому профилю.

Комплексный аспект дает возможность установить непредвзятый характер связей между классическим и цифровым профилированием, отметить имеющиеся взаимосвязи и закономерности.

Вопрос эксплуатации технологий «цифры» в раскрытии и расследовании киберпреступлений в Российской Федерации остается малоизученным. Стремительный темп развития киберпреступности опережает отклик правоприменителя на трансформацию и тенденцию раскрытия и расследования правонарушений в данной области. Специальная литература по данному вопросу аргументированно отмечает проблематику применения информационно-аналитических способов раскрытия и расследования преступлений в Российской Федерации. А потому особое значение приобретает исследование иностранного опыта и внедрение правоохранительными органами цифровых технологий в практику борьбы с киберпреступностью.

Список литературы

1. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации от 07.05.2018 № 204 // Собрание законодательства Российской Федерации. 2018. № 20. Ст. 2817.

2. Что такое цифровая экономика? Тренды, компетенции, измерение // К XX-й апрельской международной научной конференции по проблемам развития экономики и общества, доклад НИУ ВШЭ. М.: Издательский дом высшей школы экономики, 2019. 85 с.

3. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М.: Книжный мир, 2018. 416 с.

4. Ларина Е. С., Овчинский В. С. Криминал будущего уже здесь. М.: Книжный мир, 2018. 512 с.

5. Краткая характеристика состояния преступности в Российской Федерации за январь-март 2021 года // Министерство внутренних дел. URL: https://xn–b1aew.xn–p1ai/reports/item/23816756/ (дата обращения: 16.06.2021).

6. Ефремова Э. Искусственный интеллект научился делать фейковые видео // Ридус. URL: https://www.ridus.ru/news/266977 (дата обращения: 16.06.2021).

7. Мурсалиева Г. Видите призыв к суициду — срочно жмите на кнопку «Пожаловаться» // Новая газета. — 2017. – 5 марта.

8. Номоконов В. А. Возвращение личностного подхода необходимо // Личность преступника и ее криминологическое изучение / Под ред. А. И. Долговой. М.: Российская криминологическая ассоциация, 2018. С. 21–29.

9. Бутенко В. В. Актуальность использования метода профайлинг при расследовании серийных изнасилований // Актуальные вопросы юриспруденции: Материалы международной научно-практической конференции № 5. Екатеринбург, 2018. С. 50–52.

References

1. On the national goals and strategic objectives of the development of the Russian Federation for the period up to 2024: Decree of the President of the Russian Federation dated 07.05.2018 No. 204 // Collection of the legislation of the Russian Federation. 2018. No. 20. Art. 2817.

2. What is the digital economy? Trends, competencies, measurement // For the XX-th April international scientific conference on the problems of economic and social development, report of the Higher School of Economics. Moscow: Higher School of Economics Publishing House, 2019. 85 p.

3. Larina E. S., Ovchinskiy V. S. Artificial Intelligence. Big data. Crime. Moscow: Knizhnyi mir, 2018. 416 p.

4. Larina E. S., Ovchinskiy V. S. The crime of the future is already here. M .: Knizhnyi mir, 2018. 512 p.

5. Brief description of the state of crime in the Russian Federation for January-March 2021 // Ministry of Internal Affairs. URL: https: //xn–b1aew.xn–p1ai/reports/item/23816756/ (access date: June 16, 2021).

6. Efremova E. Artificial intelligence learned to make fake videos // Reedus. URL: https://www.ridus.ru/news/266977 (access date: June 16, 2021).

7. Mursalieva G. You see a call to suicide — urgently click on the "Complain"button // Novaya Gazeta. 2017. – March 5.

8. Nomokonov V. A. The return of the personal approach is necessary // Personality of the criminal and its criminological study / Ed. A. I. Debt. Moscow: Russian Criminological Association, 2018. Pp. 21–29.

9. Butenko V. V. The relevance of using the profiling method in the investigation of serial rape // Actual issues of jurisprudence: Materials of the international scientific and practical conference No. 5. Yekaterinburg, 2018. Pp. 50–52.