Известия Гомельского государственного университета
имени Ф. Скорины, № 2 (143), 2024

УДК 343.85:004.9 EDN: OEDNVJ

Цифровые технологии в противодействии преступности: перспективы использования

А.Э. Набатова

В статье рассматриваются перспективы использования цифровых технологий в противодействии преступности, дается их краткая характеристика. Автор определяет, что в связи с цифровой трансформацией преступности возникает необходимость пересмотра криминолого-криминалистических подходов по предупреждению, раскрытию и расследованию преступлений.
Ключевые слова: цифровые технологии, противодействие преступности, цифровая трансформация преступности, большие данные, искусственный интеллект, блокчейн, система социального кредита.

The article discusses the prospects for the use of digital technologies in combating crime, gives a brief description of them. The author determines that in connection with the digital transformation of crime, there is a need to revise criminological and forensic approaches to the prevention, detection and investigation of crimes.
Keywords: digital technologies, crime prevention, digital transformation of crime, big data, artificial intelligence, blockchain, social credit system.

Структура преступности за последние годы претерпевает глобальные изменения, обусловленные научно-техническим прогрессом и бурным развитием цифровых технологий. Достижения в области IT-сферы активно используются в преступной деятельности, что серьезно трансформирует криминологические подходы к предупреждению преступности и вносит коррективы в традиционное понимание таких криминалистических категорий, как время, место, способ, орудия, средства совершения преступления и т. д. В связи с заявленным тезисом рассмотрение вопросов внедрения цифровых технологий в противодействие преступности представляется весьма актуальным.

Объектом исследования в рамках статьи выступают закономерности деятельности уполномоченных субъектов по противодействию преступности с использованием цифровых технологий. *Цель* заключается в определении перспектив использования цифровых технологий в противодействии преступности с учетом уровня развития последних. Для достижения поставленной цели необходимо решить следующие *задачи*: 1) провести краткий анализ количественных и качественных показателей преступности в стране, определив цифровой компонент в ее структуре; 2) установить цифровые технологии, использование которых возможно при противодействии преступности, и дать их краткую характеристику; 3) определить перспективы их применения в криминолого-криминалистическом аспекте в целях совершенствования деятельности по противодействию преступности. В *методологию* исследования вошли системный подход, анализ, синтез, логический, социологический и статистический методы и др.

Если отталкиваться от количественных показателей зарегистрированных преступлений в Республике Беларусь, то наблюдаются следующие тенденции. В 2020 г. было зарегистрировано 95 478 преступлений, в 2021 – 87 696, в 2022 г. – 88 555, за I квартал 2023 г. – 19 596 [1], [2]. По данным Следственного комитета Республики Беларусь, количество киберпреступлений в 2020 г. составило 25 571, в 2021 – 15 503, за I квартал 2022 г. – 2 833 [3].

Анализ качественных характеристик преступности показал, что все больше деяний совершается с использованием глобальной компьютерной сети Интернет. Она, как правило, выступает местом, средством, орудием совершения преступлений при разжигании расовой, национальной, религиозной либо иной социальной вражды или розни, реабилитации нацизма, экстремизме, склонении к самоубийству, развратных действиях, понуждении к действиям сексуального характера, клевете, незаконных действиях в отношении наркотических средств, психотропных веществ, их прекурсоров и аналогов, хищении, путем модификации компьютерной информации, массовых беспорядках, заведомо ложном сообщении об опасности и т. д. Широкое распростра-

нение получили преступления, посягающие на компьютерную безопасность и связаны с модификацией компьютерной информации (ст.ст. 349, 350, 352 Уголовного кодекса Республики Беларусь (далее – УК)), разработкой вредоносных и иных программ, используемых в преступных целях (ст. 354 УК), нарушением правил эксплуатации компьютерной системы или сети (ст. 355 УК).

При изучении преступности особое место отводится личности преступника и вопросам предупредительного, профилактического воздействия на нее [4]. Приведем статистические данные (таблица 1), подтверждающие тот факт, что правоохранительные органы ежегодно сталкиваются с достаточно многочисленной группой лиц, привлекаемых к уголовной ответственности:

Таблица 1 – Качественные и количественные показатели о преступности и лицах, совершивших преступления и осужденных за их совершение в Республике Беларусь за 2020–2022 гг. [5]

Качественные характеристики	Количественные характеристики / период		
	2020	2021	2022
Лица, совершившие преступления	40734	41323	42297
Мужчины	33506	33862	33224
Женщины	7228	7461	7730
Несовершеннолетние	1270	1351	1343
Число осужденных по приговорам судов, вступивших в законную силу	34572	36356	38206

Определяя количественные показатели по лицам, осужденным и задержанным за совершение преступлений, отметим следующие тенденции. За хищения путем использования компьютерной техники и преступления против компьютерной безопасности в 2020 г. было осуждено 1539 чел., в 2021 г. – 1206. Многочисленными являются преступления против собственности (за совершение краж зарегистрировано в 2020 г. – 8760 чел., 2021 г. – 9224 чел., 2022 г. – 11524 чел.; за грабежи в 2020 г. – 1051 чел., 2021 г. – 1138 чел., 2022 – 1166 чел.; за мошенничества в 2020 г. – 736 чел., 2021 г. – 900 чел., 2022 г. – 1227 чел.). За хулиганство в 2020 г. задержано 2008 чел., в 2021 г. – 2254 чел., 2022 – 2555 чел. За преступления, связанные с незаконными действиями в отношении наркотических средств, психотропных веществ, их прекурсоров и аналогов, в 2020 г. было задержано 2002 чел., в 2021 г. – 2050 чел., 2022 г. – 2491 чел. За убийства в 2020 г. было привлечено к ответственности 293 чел., в 2021 г. – 317 чел., 2022 г. – 254. Так же, в республике зарегистрировано свыше 6 тыс. экстремистских преступлений, большая часть которых совершена в 2020–2021 г., 77 % из них раскрыто, с 2020 г. судами рассмотрено почти 3000 уголовных дел экстремистской направленности в отношении 3645 лиц. В частности, к лишению свободы по делам данной категории осуждено 42 % преступников, еще 20 % – к ограничению свободы [6].

Безусловно, наблюдаются положительные тенденции в деятельности уполномоченных субъектов по установлению лиц, совершающих преступления, раскрытию и расследованию преступлений. Однако, учитывая набирающую обороты цифровизацию, деятельность по противодействию преступности нуждается в серьезной трансформации, связанной с внедрением технологий цифрового мира: по установлению лиц, планирующих либо совершивших преступления; при раскрытии и расследовании преступлений; по разработке мер предупредительного воздействия на граждан, связанных с недопущением противоправного поведения. В пользу заявленного тезиса приведем следующие аргументы. Как уже отмечалось выше, и как показал краткий статистический анализ преступности, во-первых, достижения в области IT-технологий и научно-технического прогресса не только активно внедряются в деятельность правоохранительных органов, но и используются преступниками, существенно изменяя способы, орудия, средства совершения преступлений, и влияют на средства и методы противодействия преступности. Во-вторых, с переходом от индустриального к цифровому обществу пришло понимание того, что самым важным и стратегическим ресурсом является информация, активно используемая преступниками при совершении преступлений (например, кибермошенничество, терроризм и экстремизм, изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с участием несовершеннолетних и т. д.). В-третьих, как данность мы воспринимаем тот факт, что глобальная компьютерная сеть Интернет выступает пространством для объединения преступников в организованные группы, где осуществляется поиск жертв преступных посягательств и совершаются преступления.

В целях эффективного воздействия на цифровую трансформацию преступности целесообразно прибегнуть к более широкому применению технологий цифрового мира, адаптировать их для нужд правоохранительной деятельности. На наш взгляд, наиболее перспективными для использования являются следующие из них: 1) большие данные; 2) искусственный интеллект; 3) блокчейн технологии. В противодействии преступности указанные технологии наиболее активно применяются в США, Великобритании, Германии, Нидерландах, Японии, Китае. Особого внимания заслуживает опыт наших китайских партнеров по построению системы социального кредита своих граждан (далее по тексту – ССК), которая открывает далеко идущие перспективы по предупреждению противоправного поведения различных субъектов (отдельных граждан, социальных групп, субъектов хозяйствования и т. д.) [7]. ССК представляет собой результат использования всех выше названных цифровых технологий, используемых для формирования цифрового профиля граждан Китая [8, с. 87–89].

Итак, большие данные (big data – англ.) – информационная технология цифрового мира, серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети. Говоря о больших данных в широком смысле, можно констатировать появление технологической возможности анализировать информацию в определенных проблемных областях в мировых масштабах данных для определенных целей (например, экология, экономика, национальная безопасность и т. д.). Характеризуя большие данные, выделяют «три V»: объем (volume – англ.) – величина физического объема данных; скорость (velocity – англ.) прироста данных, а также высокоскоростная обработка данных и получение результатов; многообразие (variety – англ.) – возможность одновременной обработки структурированных, полуструктурированных и неструктурированных данных.

Источниками больших данных выступают социальные данные, генерируемые людьми в социальных сетях, глобальной компьютерной сети Интернет («Интернет вещей», «Бодинет»); GPS-данные о перемещениях; статистика о рождаемости, смертности, уровне жизни; иная информация, отражающая показатели жизни людей; сведения о банковских транзакциях; логистическая информация; веб мобильных приложений; данные систем слежения и информация, получаемая со спутников. В настоящее время разработан обширный инструментарий для обработки больших данных от интеллектуального анализа до искусственного интеллекта.

Искусственный интеллект (далее – ИИ) еще одна технология цифрового мира, получившая свое развитие с 2016 г., применяемая, в том числе, для реализации правоохранительной функции. Наиболее показательным является пример Китая, где ИИ используется в деятельности полиции, судов при отправлении уголовного правосудия [9, с. 53–54]. США, Великобритания, ОАЭ, Индия, Франция, Швеция, Россия, Беларусь не являются исключением (например, системы ИИ используются в интеллектуальных системах наблюдения указанных стран при обеспечении безопасности в аэропортах, метро, пунктах пересечения государственной границы, на объектах с массовым пребыванием людей и т. д.).

Основа ИИ – искусственная нейронная сеть – распределенный параллельный процессор, состоящий из элементарных единиц обработки информации, накапливающих экспериментальные знания и предоставляющий их для последующей обработки. Искусственная нейронная сеть – это математическая модель нервной системы биологического организма, состоящая из искусственных нейронов. Она функционирует по принципам, сходным с работой мозга (человека, насекомого, животного). Информация, сведения поступают в искусственную нейронную сеть из окружающей среды (например, из больших данных), на основе которых происходит обучение сети, формируется память, накапливается опыт (данное свойство применяется в робототехнике). Таким образом, искусственная нейронная сеть проходит два этапа в своем жизненном цикле, благодаря чему формируется ИИ. Первый этап сопряжен с обучением – сеть учится выполнять задачи для решения которых она была создана (например, распознавание лиц, речи, походки и т. д.). Второй этап – функционирование – сеть используется для выполнения задач и представляет результаты своей деятельности, при этом продолжая формировать память, накапливать опыт.

Описанная выше технология – это так называемый «слабый» ИИ, на основе которого создаются полностью автоматизированные системы, развивающиеся в последнее время очень интенсивно. «Слабый» ИИ не заменяет человека, а решает конкретные задачи, связанные с распознаванием, установлением взаимосвязей на основе матричных и статистических методов и т. п. Однако специалисты в области IT-технологий стремятся к разработке универсального, «сильного» ИИ, способного заменить человека. В настоящее время такая возможность исследуется и перспективы создания «сильного» ИИ не совсем ясны, ввиду отсутствия технологической возможности.

Блокчейн (от англ. blockchain) – непрерывная последовательная цепочка блоков, содержащих информацию. Каждый блок имеет в своем заголовке метаданные (например, уникальная контрольная сумма, время создания), а также ссылку на предыдущий блок. Содержимое блока это, как правило, список цифровых активов и команд совершенных транзакций, их объемов и адресов участников сделок. Цепочка образует децентрализованную базу данных, которая является распределенным журналом для записи операций. Выделяют публичный блокчейн; блокчейн, принадлежащий консорциуму; приватный блокчейн.

Говоря о технологии в общих чертах, можно выделить следующие характеристики. Во-первых, информацию, содержащуюся в блоках цепочки, могут получать пользователи сети, имеющие доступ к ней. Доступ открывает специальный закрытый ключ, созданный на основе криптографического алгоритма. В связи с чем хранение и передача данных в цепочке блокчейн являются защищенными и безопасными. Во-вторых, данная технология используется для разработки программного обеспечения, способного выявлять и удалять, например, террористический, экстремистский контент до его массового продвижения в компьютерной глобальной сети Интернет [9, с. 51]. В-третьих, возможности применения блокчейна в противодействии преступности обширны в силу таких свойств, как общедоступность, надежность, высокая адаптивность и рентабельность. Например, в Китае блокчейн, ИИ, большие данные используются для цифровизации правоохранительной деятельности и правосудия, в том числе при расследовании и рассмотрении уголовных дел. В частности, блокчейн технологию активно применяют для распределенного хранения доказательств в электронном формате, исключая тем самым их фальсификацию; верификации криминалистических экспертиз и финансовых документов, используемых в судебном процессе [10].

Что же касается опыта Китая по ССК граждан, то данный подход вызывает множество разноплановых дискуссий и является объектом исследования в различных научных публикациях последних лет (С.А. Буткевич, П.Н. Данилин и И.Ю. Хилько, С.Д. Галиуллина и др., П.В. Трощинский, Т.Н. Юдина и Х.С. Сулемонова). В контексте нашего исследования определим наиболее важные аспекты ССК.

ССК в Китае была заложена во времена династии Сун (960–1279 гг.). В указанный период существовала круговая порука, называемая «баоцзя». Все жители делились на группы по 5–10 семей, должны были следить друг за другом и нести коллективную ответственность за противоправное поведение членов сообщества. Новое развитие система получила при Мао Цзэдуне в 1950-х гг., путем создания учета некоторых категорий граждан. В отношении последних формировались папки с личной информацией на бумажных носителях. С развитием интернета и цифровых технологий в 2002 г. на XVI съезде КПК Генеральный секретарь Цзян Цзэминь поставил задачу создания общекитайской системы социального кредита. В настоящее время данная система повсеместно внедряется в КНР [10, с. 50–51].

Система социального кредита – это электронная рейтинговая система оценки действий отдельных физических и юридических лиц, влияющая на их дальнейшую правоспособность, в том числе дающая право на получение различных льгот и привилегий, а также ограничивающая в отдельных правах лиц, систематически совершающих антисоциальные поступки, преступления. Отметим основные элементы данной системы: 1) сведения о гражданах и юридических лицах накапливаются в цифровом формате; 2) для накопления, обработки информации, формирования рейтинга используются технологии больших данных и ИИ, сосредоточенные в государственных органах – едином информационном центре; 3) учету подлежат все граждане Китая и юридические лица, осуществляющие деятельность на его территории; 4) доступ к информации о рейтинге граждан имеют, в том числе правоохранительные органы.

В соответствии с системой социального кредита каждое лицо получает стартовый рейтинг – 1000 баллов. Они начисляются за положительные действия (сообщение о правонарушении, своевременная оплата коммунальных платежей в течение года, активная волонтерская и иная общественная деятельность и т. д.), либо негативные действия (несвоевременная оплата коммунальных платежей, нарушение правил дорожного движения, курение в запрещенных местах, использование поддельных документов, распространение ложной информации о терроризме, совершение преступлений и т. д.). Таким образом, рейтинг рассчитывается путем анализа 160 000 параметров. В его основу положены четыре основных критерия: честность в государственных делах; коммерческая добросовестность; поведение в обществе; судебная история. После обработки данных гражданам присваиваются баллы: AAA (1050 баллов), AA (1000 баллов), A, B (900 баллов) – образцовые жители Китая; C (менее 849 баллов) – «неблагонадежные» жители (например, не имеют права занимать должности в органах государственной и муниципальной службы); D (менее 600 баллов) – наихудший рейтинг.

Для лиц, имеющих высокий рейтинг, открываются широкие возможности. Лица, которым присваивается рейтинг D, подвергаются различным ограничениям (например, они не могут свободно передвигаться по стране, их трудоустройство затруднено, им отказано в социальном обеспечении, запрещается обучение в престижных школах и вузах, получение кредитов и т. д.) и контролю со стороны правоохранительных органов.

На основании краткого анализа цифровых технологий в противодействии преступности представляется возможным определить некоторые перспективы их использования.

Как представляется, есть все основания по применению технологии больших данных в рамках криминалистической регистрации путем интеграции учетов Информационного центра МВД, ГКСЭ Республики Беларусь и других ведомств в единую систему, позволяющую осуществлять интеллектуальный анализ разрозненной информации по запросу в процессе раскрытия и расследования преступлений.

Большие данные в совокупности с ИИ способны усилить с технологических позиций методологию учения о криминалистической идентификации, криминалистическую трасологию, дактилоскопию, криминалистическую габитоскопию в части развития комплексных цифровых систем, способных в режиме реального времени проводить идентификацию граждан по биометрическим данным (отпечаткам пальцев и ладоней рук, изображениям лиц и радужной оболочки глаза, татуировкам, шрамам, голосу, походке и др.) или прогнозировать их поведение.

Перечисленные технологии могут быть успешно применены в рамках криминалистической тактики и методики и вывести на новый технологический уровень: планирование расследования; принятие управленческих решений; выдвижение и проверку версий; разработку профилактических, предупредительных мер и их реализации в целях предупреждения преступности; прогнозирование и разрешение следственных ситуаций; проведение следственных действий путем анализа их результатов и устранения противоречий, в том числе по многоэпизодным уголовным делам; оценку достаточности собранных доказательств для предъявления обвинения и последующего расследования уголовного дела и т. д.

Блокчейн технологии будут полезны для совершенствования криминалистической тактики и методики и выведут на новый технологический уровень деятельность по собиранию, оценке, использованию и хранению доказательств в электронном формате при расследовании преступлений.

Опыт Китая по ССК граждан носит дискуссионный характер и вызывает множество вопросов по обеспечению прав и законных интересов граждан, но, безусловно, представляет научный и практический интерес в условиях цифровизации. ССК может рассматриваться как базис для выстраивания системы предупредительных мер в противодействии преступности и удержании ее под должным социальным контролем.

Внедрение ССК влечет пересмотр криминологических парадигм, устоявшихся в теории предупреждения преступности, а также совершенствование правоприменительной практики по предупредительному воздействию на личность преступника и преступность в целом.

Учитывая тот факт, что граждане нашей республики, как и граждане Китая, в большинстве своем законопослушные и дисциплинированные, придерживаются устоявшихся традиций, внедрение подобного опыта представляется весьма перспективным для нашей страны с учетом национальной правовой модели, социально-экономического и научно-технического развития.

Литература

1. Численность лиц, совершивших преступления [Электронный ресурс] / Национальный статистический комитет. – Режим доступа : http://dataportal.belstat.gov.by/Indicators/Search?code=1063066. – Дата доступа : 10.07.2023.

2. Количество зарегистрированных преступлений за I полугодие 2022 г. [Электронный ресурс] / МВД. – Режим доступа : https://www.mvd.gov.by/ru/page/statistika. – Дата доступа : 10.07.2023.

3. Число киберпреступлений снизилось почти вдвое. Заместитель предстедателя СК о тенденциях в области IT-преступлений [Электронный ресурс] / БЕЛТА. – Режим доступа : https://www.belta.by/society/view/chislo-kiberprestuplenij-snizilos-pochti-vdvoe-zampred-sk-o-tendentsijah-v-oblasti-it-prestuplenij-496880-2022/. – Дата доступа : 10.07.2023.

4. Личность преступника : характеристика, предупреждение формирования и криминализации : в 2 ч. / В. А. Ананич [и др.] ; под общ. ред. В. А. Ананича. – Минск : Академия МВД, 2022. – Ч. 1 : Общенаучные и теоретико-правовые основы изучения личности преступника. – 324 с.

5. Статистический ежегодник Республики Беларусь / Национальный статистический комитет Республики Беларусь. – Минск, 2022. – С. 148–154.

6. Швед : количество экстремистских преступлений в прошлом году значительно уменьшилось [Электронный ресурс] / БЕЛТА. – Режим доступа : https://www.belta.by/society/view/shved-kolichestvo-ekstremistskih-prestuplenij-v-proshlom-godu-znachitelno-umenshilos-551705-2023/. – Дата доступа : 10.07.2023.

7. Рувинский, Р. З. «Система социального кредита» : исторические предпосылки и доктринальные основания феномена [Электронный ресурс] / Р. З. Рувинский, А. А. Тарасов // Национальная безопасность / nota bene. – 2020. – № 3. – Режим доступа : https://nbpublish.com/library_read_article.php?id=33021. – Дата доступа : 10.07.2023.

8. Разумов, Е. А. Цифровое диктаторство : особенности системы социального кредита в Китайской Народной Республике / Е. А. Разумов // Труды ИИАЭ ДВО РАН. – 2019. – Т. 24, № 3. – С. 86–97.

9. Антонян, Е. А. Вопросы применения новых технологий в противодействии кибертерроризму / Е. А. Антонян // Мониторинг правоприменения – 2020. – №1 (34). – С. 51–55.

10. Трощинский, П. В. Цифровой Китай до и в период коронавируса : особенности нормативно-правового регулирования / П. В. Трощинский // Право и цифровая экономика. – 2021. – № 1 (11). – С. 44–58.

Гомельский государственный
университет имени Франциска Скорины

Поступила в редакцию 07.09.2023