УДК 343.85:004
DOI 10.17150/2500-4255.2018.12(6).753-766

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ, ЕЕ ПРОГНОЗИРОВАНИИ, ПРЕДУПРЕЖДЕНИИ И ЭВОЛЮЦИИ

А. П. Суходолов[1], А. М. Бычкова[2]
[1] Байкальский государственный университет, г. Иркутск, Российская Федерация
[2] Ассоциация юристов России, г. Иркутск, Российская Федерация

Информация о статье
Дата поступления
30 августа 2018 г.
Дата принятия в печать
15 ноября 2018 г.
Дата онлайн-размещения
24 декабря 2018 г.

Ключевые слова
Искусственный интеллект; глубинное обучение; большие данные; цифровая криминология; современные технологии противодействия преступности

Аннотация. Прогнозирование преступности, ее предупреждение и противодействие ей с использованием современных технологий, по мнению авторов, должны стать приоритетной задачей государства наряду с развитием экономики, образования, медицины, усилением обороноспособности страны. В статье раскрыты понятия «искусственный интеллект», «машинное обучение», «большие данные», «глубинное обучение», «нейронные сети» с точки зрения их использования как преступностью, так и правоохранительными органами и судами. Рассмотрено применение технологий, основанных на искусственном интеллекте, высокотехнологичной преступностью (фишинг, дроны, фейковая информация, боты и др.). Охарактеризованы основанные на искусственном интеллекте современные программные решения, направленные на противодействие преступности: программы для анализа большого объема данных, обработки потокового видео, распознавания внешности, платформы контекстного поиска и т. д. Описаны существующие ресурсы, используемые для предиктивной аналитики (в частности, межведомственная экспериментальная программа «Искусственный интеллект в расследовании и оперативно-розыскной деятельности при совершении уголовных преступлений»; программа распознавания людей по фрагментам татуировок; программа распознавания по фотографиям и потоковому видео людей, осуществивших пластические операции, и выдачи вариантов их первоначальной внешности; платформа контекстного интеллекта Nigel; система Mayhem и др.), и их возможности в прогнозировании как преступности в целом, так и индивидуального преступного поведения. Обозначены этические дилеммы, связанные с принятием искусственным интеллектом правовых решений в отношении конкретных индивидов. Приведены примеры применения искусственного интеллекта для профилактики преступности (программа COMPAS, система прогнозной психометрики преступного сообщества, программа Harm Assessment Risk Tool, аналитический программный комплекс CEG, система прогнозирования преступлений PredPol, система ePOOLICE, программные продукты Palantir, российская система «Искусственный интеллект»). Обозначены индикаторы системы раннего предупреждения преступности: показатели совпадения, запаздывающие, циклические и контрциклические индикаторы. Констатировано отставание России от других стран в использовании искусственного интеллекта в правоохранительной сфере и предложено принять Современную стратегию противодействия преступности, ее прогнозирования и предупреждения. Указаны возможные направления данной стратегии.

ARTIFICIAL INTELLIGENCE IN CRIME COUNTERACTION, PREDICTION, PREVENTION AND EVOLUTION

Alexander P. Sukhodolov[1], Anna M. Bychkova[2]
[1] Baikal State University, Irkutsk, the Russian Federation
[2] Association of Russian Lawyers, Irkutsk, the Russian Federation

Article info
Received
2018 August 30

Abstract. Crime prediction, prevention and counteraction with the use of modern technologies should, according to the authors, become a priority task for the state, along with the development of economy, education, medicine and the enhancement

ISSN 2500-4255

Accepted
2018 November 15
Available online
2018 December 24

Keywords
Artificial intelligence; deep learning; big data; digital criminology; modern technologies of counteracting crime

of defense capacity. The article describes the concepts of «artificial intelligence», «machine learning», «big data», «deep learning», «neural networks» from the standpoint of how they are used both by criminals and by law enforcement bodies and courts. The authors examine the application of technologies which use artificial intelligence, hi tech crime (fishing, drones, fake information, bots, and so on). They outline modern software solutions based on artificial intelligence and aimed at counteracting crime: software that analyzes big volumes of data, processing of stream videos, facial recognition, contextual searching platforms, etc. The authors also describe the existing resources for predictive analytics (in particular, inter-agency experimental software «Artificial Intelligence in Police Work and Investigation of Criminal Offences»; software for recognizing people based on fragments of their tattoos; facial recognition of people after plastic surgeries in pictures and stream videos, with the generation of variants of their original appearance; platform of contextual intelligence Nigel; system Mayhem and others) and how they can be used to predict both crimes in general and individual criminal behavior. The authors also outline ethical dilemmas connected with legal decisions made by artificial intelligence regarding specific people. They present examples of using artificial intelligence for crime prevention (software COMPAS, criminal community's psychometric prediction system, Harm Assessment Risk Tool, analytical software complex CEG, crime prediction system PredPol, ePOOLICE system, Palantir software, Russian system «Artificial intelligence»). They also outline the indicators of the early crime prevention system: indicators of matching, lagging, cyclical and counter-cyclical indicators. The authors state that Russia is lagging behind other countries in its use of artificial intelligence in law enforcement and suggest adopting the Modern Strategy of Crime Counteraction, Prediction and Prevention. Possible directions of this strategy are described.

Начало информационно-цифровой революции связано с появлением электронно-вычислительных машин. Несмотря на то что человек вводит соответствующие программы и формулирует задачи, ЭВМ самостоятельно оперируют цифрами, накапливают, генерируют и передают новую информацию, в том числе такую, какую ни человек, ни человечество в целом не смогли бы получить своими силами.

Особенно заметно это проявилось с возникновением систем *искусственного интеллекта*: все бóльшие классы задач ЭВМ ставят перед собой сами и решают их относительно автономно, без участия человека. «Как ребенок, овладевший грамотой, в дальнейшем умеет самостоятельно читать и писать, так и современные ЭВМ могут считывать, генерировать и передавать цифровую информацию как человеку, так и себе подобным, — отмечает экономист С. Ю. Глазьев. — Для общения с человеком они умеют преобразовывать цифру в звуки, слова и символы, сообщая и принимая информацию от человека. Общение с себе подобными идет на цифровом языке без участия человека, запрограммировавшего компьютерную систему на выполнение тех или иных функций или решение определенных задач» [1, с. 31].

Рождение искусственного интеллекта как научного направления связывают с 1940-ми гг., когда Норберт Винер опубликовал свои основополагающие работы по кибернетике. Собственно термин «искусственный интеллект» (англ. artificial intelligence) был предложен в 1956 г. в Дартмутском колледже (США) на семинаре с одноименным названием, где был выдвинут ключевой тезис: «Каждый аспект обучения или любая другая особенность интеллекта могут быть в принципе так точно описаны, что машина сможет сымитировать их» [2].

Система искусственного интеллекта — это программная система, имитирующая на компьютере процесс мышления человека. Искусственный интеллект представляет собой направление информатики, целью которого является разработка аппаратно-программных средств, позволяющих пользователю-непрограммисту ставить и решать свои традиционно считающиеся интеллектуальными задачи, общаясь с ЭВМ на ограниченном подмножестве естественного языка [3, с. 5].

Информационные подразделения ФБР совместно с лабораторией искусственного интеллекта корпорации Google выработали следующее инженерное определение искусственного интеллекта: «Искусственный интеллект — это программно-аппаратный комплекс, обеспечивающий поддержку и/или принятие результативных решений в динамичной, неустойчивой среде в установленное время на основе заведомо неполной, нечеткой и не имеющей пол-

ной доказательственной базы информации». В. С. Овчинский и Е. С. Ларина пишут, что именно данное определение положено в разработку концепции архитектуры и перечня программных решений ФБР [4, с. 15].

В последнее время понятие «искусственный интеллект» упоминается наряду с такими терминами, как «большие данные» (Big Data), «машинное обучение», «глубинное обучение» и «нейронные сети».

Большие данные, согласно терминологии ООН, представляют собой «накопление и анализ значительно возросшего объема информационных ресурсов, который повышает возможности их хранения и анализа с использованием созданных ранее аппаратных и программных средств» [там же, с. 129]. Появление больших данных стало возможным благодаря расширению возможностей хранения данных и круга имеющихся в наличии их источников, в число которых входят данные спутниковых изображений, сетей мобильной телефонной связи, социальных сетей и сканирующих устройств [там же, с. 130–132].

Машинное обучение — одно из направлений искусственного интеллекта, основной принцип которого заключается в том, что машины получают данные и «обучаются» на их основе. В настоящее время это наиболее перспективный инструмент для бизнеса, науки и сферы принятия важных управленческих решений. Системы машинного обучения позволяют быстро применять знания, полученные при обучении на больших наборах данных, за счет чего преуспевают в таких задачах, как распознавание лиц, речи, объектов, перевод, и многих других. В отличие от программ с закодированными вручную инструкциями для выполнения конкретных задач, машинное обучение дает системе возможность научиться самостоятельно распознавать шаблоны и делать прогнозы [2].

Глубинное обучение является подмножеством машинного обучения. Оно использует некоторые методы машинного обучения для решения реальных задач, применяя нейронные сети, которые могут имитировать принятие решений человеком.

Нейронные сети возникли в результате исследований в области искусственного интеллекта, в ходе которых появилась идея воспроизвести способность биологических нервных систем обучаться и исправлять ошибки, моделируя низкоуровневую структуру мозга. Теория искусственных нейронных систем зародилась в 1940-х гг., и спустя уже 20 лет были разработаны однослойные нейронные системы (*перцептроны*), которые в ряде случаев оказались способны обучаться, осуществлять предсказания и распознавать образы. К 1980-м гг. в этой области произошел прорыв благодаря революционным работам Джона Хопфилда и Тейво Кохонена. Многослойные нейронные сети нового поколения успешно справлялись с задачами, недоступными для перцептронов [3, с. 112–113].

Элементарная база позволила создать мощные нейрокомпьютеры и программные нейропакеты для распознавания образов, текстового поиска, поиска изображений, перевода, прогнозирования, обнаружения спама, мошенничества и решения ряда других задач, в которых входные данные были неполны, зашумлены и даже противоречивы.

Качество глубинного обучения зависит от величины массивов данных для обучения, так как существует огромное количество параметров, которые необходимо настроить для алгоритмов обучения, чтобы избежать ложных срабатываний. При недостаточности входных данных глубинное обучение может выдавать ошибочные результаты. Например, система распознавания лиц Google на первых этапах запуска помечала много темнокожих лиц как «горилл». «Это пример того, что произойдет, если у вас нет афроамериканских лиц в вашем наборе обучения, — поясняла Anu Tewary, главный специалист по работе с данными Mint at Intuit. — Если у вас нет афроамериканцев, работающих над системой, если у вас нет афроамериканцев, тестирующих систему, то, когда ваша система сталкивается с афроамериканскими лицами, она не будет знать, как вести себя» [2].

Теоретические, практические и этико-правовые аспекты использования искусственного интеллекта в противодействии преступности широко освещаются в работах зарубежных авторов[1] [5–13], а с недавних пор — и в отечественных исследованиях [14–17]. Неоценимый вклад в познание возможностей современных технологий внесли В. С. Овчинский и Е. С. Ларина [4; 18–23], рассматривающие искусственный интеллект как технологию тройного назначения, которая может быть использована для гражданских, военных и криминальных целей [21, с. 374]. Отличитель-

[1] Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities // International Criminal Justice Review. 2004. Vol. 14, iss. 1. DOI: 10.1177/1057567704014001127.

ной особенностью современной преступности является ее способность брать на вооружение передовые технологические решения, что обусловлено как ее безграничными финансовыми возможностями, так и определенной прозрачностью научных достижений: «Злоумышленники могут беспрепятственно приобрести как программные, так и аппаратные компоненты самых мощных систем искусственного интеллекта. Широкое использование открытого кода позволяет преступникам без затрат получать доступ к последним разработкам ведущих компаний. В связи с тем что над алгоритмами искусственного интеллекта работают не закрытые коллективы специалистов, а открытые сообщества программистов, преступники имеют возможность бесплатно получать новейшие разработки. Попытки Министерства внутренней безопасности США законодательно ограничить распространение определенных разработок в области искусственного интеллекта не привели к успеху, так как программисты просто отказались закрыть для себя возможность создавать системы с открытым программным кодом» [4, с. 34].

Изучение современной высокотехнологичной преступности позволяет выделить следующие способы и сферы использования преступниками искусственного интеллекта (табл. 1).

Фишинг (англ. fishing — рыбная ловля, выуживание) представляет собой вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя — логинам и паролям. Массовые рассылки электронных писем от имени популярных брендов и личных сообщений внутри различных сервисов (чаще всего банков и социальных сетей) со ссылками на сайт, внешне неотличимый от настоящего, приводят к тому, что некоторые пользователи при переходе на поддельную страницу вводят свои логины и пароли, используемые для доступа к определенному сайту, в результате чего мошенники получают доступ к аккаунтам и банковским счетам своих жертв.

Создание комбинированных систем, объединяющих искусственный интеллект с роботизированным устройством, также в буквальном смысле слова взято на вооружение преступниками. К примеру, дроны, связанные с искусственным интеллектом, являющимся центром управления ими, применяются как государственными структурами (в ходе боевых действий и при выполнении других задач), так и преступными организациями (контрабанда наркотиков и иных запрещенных веществ, доставка различных предметов в места лишения свободы). Наркокартели из Мексики отправляют свой товар в США при помощи беспилотников с заранее введенными данными GPS, что полностью отменяет необходимость услуг не только курьера, но и оператора [4, с. 37]. Дроны со взрывчаткой использовались

Таблица 1 / Table 1

Использование искусственного интеллекта в совершении преступлений и других противоправных действий

Using artificial intelligence to commit crimes and other unlawful acts

Способ совершения преступления / Means of committing a crime	Сфера применения / Sphere of use
Фишинг	Посягательства на собственность, неприкосновенность частной жизни, тайну переписки, хакерские атаки
Использование дронов	Посягательства на жизнь, теракты, слежка, несанкционированная съемка, изучение объектов недвижимости с целью последующего проникновения, контрабанда наркотиков и других предметов, запрещенных или ограниченных в обороте, перемещение наркотиков, оружия, денег и пр. в места лишения свободы
Синтезирование фейковой информации	Дискредитация лиц, принимающих решения, шантаж, провоцирование паники
Использование автоматизированных автономных систем, управляемых искусственным интеллектом	Посягательства на жизнь и здоровье, слежка
Использование ботов	Мошенничество, распространение наркотиков, порнографии, побуждение к самоубийству, посягательства на половую неприкосновенность

при покушении на убийство президента Венесуэлы Николаса Мадуро 4 августа 2018 г. [24].

Дроны стали применяться для слежки за агентами и сотрудниками правоохранительных органов, за свидетелями преступлений и членами конкурирующих преступных группировок, а также в поисках объектов для краж и ограблений, с целью слежения за контейнерами с контрабандным товаром и съемок интимных встреч для дальнейшего шантажа.

Прогресс в области искусственного интеллекта и новейшие технологии порождают новые угрозы, к примеру хакерские атаки, которыми будет управлять не человек, а искусственный интеллект, распространение дезинформации и фейков [25; 26].

Элементы искусственного интеллекта используются в качестве способа компенсации низкой квалификации людей: так, активное применение наводящихся с использованием искусственного интеллекта снайперских винтовок дальнего действия, имеющих джойстики для управления, заметно снижает требования к профессиональной подготовке боевиков [4, с. 45].

Наблюдается процесс автоматизации *социальной инженерии*[2], примером чего являются так называемые боты. *Бот* (сокр. от «робот») — это программа, способная по определенному алгоритму выполнять какие-либо действия через интерфейсы, предназначенные для людей, например вести диалог с посетителями форума либо в соцсети.

Беспрецедентная атака ботов, зазывающих пользователей в печально известные «группы смерти», была отмечена в 2017 г. в социальной сети «ВКонтакте». В марте 2017 г. руководитель отдела модерации «ВКонтакте» И. Коренев сообщил, что с начала января на сайте этой соцсети было сгенерировано около 3 млн сообщений с хештегами и стишками, возможно, призывающими к суициду. Подобные сообщения при этом постоянно менялись, размывались какими-либо символами. Руководство «ВКонтакте» увидело за таким всплеском «целенаправленную атаку ботов», что было очевидно, так как «в этот период появилось несколько тысяч страниц, созданных исключительно для того, чтобы публиковать такие хештеги» [29].

Специалисты Центра исследований легитимности и политического протеста провели анализ страниц, с которых пошла новая волна стихотворений с хештегом, выяснили время запуска стихов, а также использованные для этого аккаунты. Анализ аккаунтов позволил сделать вывод, что имела место автоматизированная рассылка стихов по страницам «ВКонтакте». Большинство рассылок выявлено на устройствах, работающих под операционной системой Android, программой рассылки оказалась VK iHA bot. Этот робот появился в Сети в 2014 г., его следы привели к жителю Киева, известному под ником Dr. Failov. Так как его программа написана для Android-устройств, то она была и на Google Play, где указаны почта и сайт разработчика, а также страна регистрации — Украина.

Dr. Failov известен как создатель вредоносных программ, к примеру программы вируса-вымогателя «Файло4кА». В зависимости от версии «Файло4кА» создает разное количество файлов, их типов и разрешений, захламляет операционную систему и вызывает неисправности компьютера. Потребителю предлагается использовать «Файло-4кУ» как, скажем, розыгрыш. В последних версиях программы все настолько автоматизировано, что при желании ее можно моментально удалить с компьютера, но только с помощью секретного кода, получить который можно за деньги.

Раскрытая схема ботов показала, что вовлечение подростков в «игру» производилось в автоматическом режиме программными средствами. Робот сам мог вести диалог с пользователями, отвечая на стандартные вопросы и распознавая сленг молодежной аудитории. Машина предлагала написавшему подростку сделать выбор («Если да, напишите 1, если нет, напишите 0»), таким образом отсеивая других ботов и допуская несовершеннолетнего на следующий уровень в «игре». В результате сначала один робот делал посев стиха, сам фильтровал его и находил посты реальных подростков. Все эти действия робот совершал через так называемое API VK (англ. application programming interface). Внутри API есть функция автоматического размещения записей, которую и использовал данный бот. Человек-куратор, купивший бота, подключался к работе с уже готовыми к серьезной «игре» подростками [30].

Продвинутым вариантом социальной инженерии является ситуация, когда человек, участвующий в диалоге с ботом, уверен, что общается с человеком, поскольку программа способна обратиться к пользователю-человеку и поддерживать с ним беседу, оперируя такими репликами, которые человек-собеседник сочтет

[2] Социальная инженерия — совокупность психологических методов и технологий воздействия на собеседника, максимально эффективно приводящих к необходимому результату [27; 28].

естественными. То есть эта программа способна оправдать ожидания человека-собеседника, она «социализирована», ведет диалог в рамках, принятых в данном обществе, ориентирована разработчиками на побуждение человека к выполнению определенных действий, что и является критерием ее успешности. Так, на одном из закрытых форумов программисты поделились опытом создания двух ботов, один из которых должен был провоцировать женщин делиться с мнимым собеседником интимными фотографиями, а второй должен был убедить собеседника пожертвовать некую сумму (до 5 дол.), переведя ее на счет через систему PayPal. Целевой аудиторией первого бота выступили англоязычные белые жительницы Восточного побережья США в возрасте от 20 до 30 лет, из которых поделились с ботом интимными снимками 4 %. В среднем уговоры занимали 16 тыс. знаков со стороны бота, причем уже после 5 тыс. знаков становилось понятно, будет ли достигнута цель, и заведомо неуспешные диалоги обрывались для экономии ресурсов. Программу обучили на выборке из 200 живых диалогов с реальными людьми, после чего она самообучилась еще на 2 тыс. диалогов и вышла на стабильный 4-процентный результат, что считается достаточно высоким достижением для программы-бота.

Бот, подготовленный для сбора «пожертвований», после запуска в Сеть собрал за сутки 15 тыс. дол. Создатели бота заявили, что сделали его не с целью наживы, а для проверки возможностей социального хакинга (перен. «взлом»), потому что, по сути, это и есть хакинг человеческого сознания, проводимый социальными методами [31].

Впрочем, человек, участвующий в диалоге с ботом, может и осознавать, что он общается с программой. Чаще всего боты используются при покупке-продаже наркотиков бесконтактным способом: бот отвечает, какие наркотики имеются в интернет-магазине, по какой стоимости реализуются, как произвести оплату и где можно «поднять закладку». В последнее время популярной площадкой для такого рода распространения становится Telegram.

Рассмотренные примеры свидетельствуют о том, что преступления, совершенные с использованием технологий искусственного интеллекта, отличает высокая степень анонимности, а иногда, как в случае с ботами, практически выводит личность правонарушителя из процесса преступных взаимодействий, что не может не порождать ощущения безнаказанности. К. Н. Евдокимов выделяет также такую характеристику технотронной преступности, как неконтролируемость, и выдвигает научную (частную) теорию «анекселенктотичной технотронной преступности» (ανεξέλεγκτος, anexélenktos, в переводе с гр. — неконтролируемый, неуправляемый; технотронный в переводе с англ. — связанный с технотроникой, т. е. техникой с использованием электроники, оказывающей влияние на развитие общества), иначе говоря, возникновения «преступности нового поколения, основанной на использовании IT-технологий, пришедшей на смену традиционной компьютерной преступности и вышедшей из-под контроля личности, общества и государства в силу своей социальной латентности, технической сложности и многогранности» [32, с. 39].

В то же время нельзя говорить о том, что только преступность берет на вооружение современные программно-технологические достижения. Имеется немало примеров различных программных решений с использованием искусственного интеллекта, направленных на противодействие преступности и ее профилактику (табл. 2).

Таблица 2 / Table 2

Искусственный интеллект в противодействии преступности
Artificial intelligence in counteracting crime

Наименование программы (эксперимента), дата и место разработки и применения / Name of program (experiment), date and place of development and use	Цели и результаты / Goals and results
Аналитические средства для правоохранительных органов i2 (США, IBM, 2001 г. — н. в.)	*Цель*: получение быстрого доступа к информации, накопленной правоохранительными органами США, для выявления в ней скрытых связей между людьми, местами, автомобилями, мобильными телефонами и т. д. *Результат*: с 2007 по 2011 г. полиции Северной Каролины удалось снизить количество совершаемых преступлений на 50 % [19, с. 44]

Окончание табл. 2 / End of the table 2

Наименование программы (эксперимента), дата и место разработки и применения / Name of program (experiment), date and place of development and use	Цели и результаты / Goals and results
Межведомственная экспериментальная программа «Искусственный интеллект в расследовании и оперативно-розыскной деятельности при совершении уголовных преступлений» (США, 2013–2016 гг.)	*Цель*: освобождение полицейских от рутинной работы, связанной с заполнением объемной документации по делу. Вместо этого полицейские диктовали все необходимое электронному помощнику, после чего программа Watson формировала стандартные отчеты и создавала условно структурированные базы. *Результат*: программа закрыта из-за неудовлетворительных результатов (Watson не справилась с оценкой качества отчетов, исключение интерактивности при составлении отчетов привело к существенному ухудшению качества работы) [4, с. 105–107]
Эксперимент, связанный с обработкой суперкомпьютером потокового видео, поступающего от всей системы видеокамер (США, 2014–2015 гг.)	*Цель*: уменьшение потребности в патрулировании городов полицейскими экипажами за счет повышения ситуационной осведомленности о месте нахождения нарушителей. *Результат*: увеличение числа задержаний нарушителей в течение первого полугодия эксперимента, но ухудшение показателей по истечении года с момента его начала вследствие того, что преступники при совершении преступлений стали принимать во внимание возможность ухода от видеонаблюдения [там же, с. 107–108]
Программа распознавания по фрагментам татуировок (США, 2014 г. — н. в., разработчики — ФБР, Cyrcadia и CureMetrix)	*Цель*: использование вариантной графической базы в качестве фильтра при автоматическом распознавании образов в потоковом видео, поступающем с городских камер видеонаблюдения *Результат*: задержание 17 лиц, находившихся в розыске [там же, с. 109–110]
Программа распознавания по фотографиям и потоковому видео людей, осуществивших пластические операции, и выдачи вариантов их первоначальной внешности (США, DOIL COGNITIVE COMPUTING, 2015 г. — н. в.)	*Цель*: выявление находящихся в розыске лиц, изменивших внешность. *Результат*: в ходе испытаний программа успешно распознала по фотографиям факт пластической операции в 97 % случаев, в потоковом видео — в 90 %, в более чем 80 % случаев успешного распознавания позволяла восстановить первоначальную внешность [там же, с. 111]
Платформа контекстного интеллекта Nigel (США, 2017 г. — н. в.)	*Цель*: контекстное распознавание ситуации (например, родитель ведет собственного упирающегося ребенка или похититель украл ребенка). *Результат*: экспертные советы правоохранителям, привязанные к уникальной конкретной обстановке [там же, с. 112–113]
Система Mayhem (США, ФБР совместно с компанией ForAllSecure и университетом штата Пенсильвания, 2017 г. — н. в.)	*Цель*: распознавание индивидуального почерка хакеров и хакерских группировок, обнаружение атак, активное тестирование и преследование хакеров вплоть до установления их локации. *Результат*: на конференции по кибербезопасности Blac Hat в 2016 г. в состязании между хакерами и Mayhem система успешно распознала четырех хакеров из пяти [там же, с. 113–114]

В. С. Овчинский и Е. С. Ларина приводят данные Интерпола и Европола, согласно которым более чем в 70 странах мира полицейские на практике используют те или иные данные *предиктивной аналитики*, опираясь на программные средства более чем 25 корпораций-производителей [4, с. 114]. Предиктивная, или предсказательная, аналитика представляет собой совокупность методов анализа данных, направленных на прогнозирование поведения людей (табл. 3).

Принятие серьезных, нередко судьбоносных для человека решений в результате алгоритми-

ISSN 2500-4255

Таблица 3 / Table 3

Искусственный интеллект в прогнозировании преступности
Artificial intelligence in predicting crime

Наименование программы, разработчики, страна, годы внедрения и использования / Name of the program, developers, country, years of installment and use	Область применения / Sphere of use
Программа COMPAS (Массачусетский технологический институт, США, 2014 г.)	Рекомендации по выбору для обвиняемых, ожидающих суда, залога или заключения под стражу; решение вопросов об условно-досрочном освобождении [4, с. 70]
Система прогнозной психометрики преступного сообщества (планируется внедрить с 2019 г. в Лионе, Франция)	Моделирование конкретных профилей преступников и прогнозирование динамики их психического состояния [там же, с. 116–117]
Программа Harm Assessment Risk Tool (2017 г., Дарем, Англия)	Выбор между содержанием под стражей или применением альтернативных мер пресечения, основанный на алгоритме искусственного интеллекта. Тестирование показало: алгоритм мог предсказать, что задержанный не представляет опасности, в 98 % случаев и верно определял находившихся в группе высокого риска в 88 % случаев [19, с. 48–49]
Аналитический программный комплекс CEG (Джексонсвилл, Александрия, Мемфис и Детройт, США, 2016 г. — н. в.)	Использование элементов искусственного интеллекта для прогнозирования скачкообразного увеличения числа возможных правонарушений в масштабах вплоть до квартала конкретного города. Для каждой локации устанавливается 45–50 параметров риска, каждый из которых имеет количественную меру. При определенных изменениях системы параметров в тех или иных кварталах или районах города резко возрастает вероятность скачкообразного увеличения количества преступлений. Параметры рассчитываются на основе первичной информации, в том числе данных с видеокамер, сообщений в социальных сетях, прогнозах погоды и т. п. В первом полугодии 2016 г. в городах, где была внедрена система, по сравнению с контрольными городами, т. е. примерно аналогичными по численности и криминогенной обстановке, удалось снизить число преступлений на 14 %, что считается большим достижением, поскольку снижение преступности на 3–4 % в год для городов с тяжелой криминогенной обстановкой считается несомненным успехом [4, с. 108–109]
Система прогнозирования преступлений PredPol (Калифорнийский университет, США, с 2014 г. применятся в США и Великобритании)	Система оснащает полицейские патрули электронными картами с мигающими красными квадратами, обозначающими места возможной противоправной активности. Специальные испытания, проводившиеся в течение почти двух лет в трех территориальных подразделениях полиции Лос-Анджелеса, доказали, что PredPol верно предугадывает в два раза больше мест преступлений, чем позволяют лучшие из существующих методик [19, с. 45–47]
Система ePOOLICE ((**e**arly **P**ursuit against **O**rganized crime using envir**O**nmental scanning, the **L**aw and **I**ntelligen**CE** systems), Евросоюз, 2013 г. — н. в.)	Система сканирования данных, изучающая страницы сайтов, электронную переписку, полицейскую информацию в поисках свидетельств деятельности организованной преступности и для оценки риска проявления нелегальной активности. Для формального анализа организованной преступности используется видео-, текстовый контент и финансовые данные [4, с. 244–291]
Программные продукты Palantir Technologies, Inc. (США, 2003 г. — н. в.)	Аккумуляция данных ДНК, записей систем видеонаблюдения, телефонных переговоров, радиоперехватов, данных о передвижениях, сообщений в СМИ, информации из соцсетей, сведений от информаторов, транзакциях, сопровождающих преступления, прежде всего террористического характера. Программное обеспечение Palantir доказало свою результативность в раскрытии преступных сетей по подготовке терактов, в розыске педофилов и т. д. [19, с. 57–58]
Система «Искусственный интеллект» («Объединенная приборостроительная корпорация», Россия, тестируется с 2016 г.)	Фиксация нарушений на границах России с помощью инфракрасных датчиков, сейсмосенсоров, радиолокационных устройств с целью наработки базы данных для дальнейшего компьютерного анализа информации о нарушении границ, дистанционного контроля ситуации и прогнозирования опасностей [там же, с. 74–76]

ческих вычислений искусственного интеллекта вызывает немалые опасения. Так, В. С. Овчинский и Е. С. Ларина описали этическую проблему, связанную с внедрением в США программы с элементами искусственного интеллекта COMPAS. Она применяется во многих судах штатов для принятия решения, рекомендовать ли ожидающим суда присяжных тюремное заключение или освобождение под залог. Программа положительно зарекомендовала себя, и ее стали использовать также при решении вопросов об условно-досрочном освобождении. Однако когда портал Propublica.org, который является площадкой сообщества ученых, негативно относящихся к искусственному интеллекту, расшифровал черный ящик системы COMPAS, выяснилось следующее. Оказалось, что система априори уменьшает шансы на освобождение под залог и условно-досрочное освобождение для лиц латиноамериканского происхождения, не имеющих легального статуса на территории США, а также для афроамериканцев с доходом выше прожиточного минимума, но ниже, чем у среднего класса. Если первый вывод был интуитивно понятен, то второй породил всеобщее недоумение, и эксплуатация системы после широкого общественного резонанса была приостановлена.

Создатели программы COMPAS предложили проекту Propublica создать независимую группу — своего рода первый в истории Америки алгоритмическо-статистический суд, которым руководил математический директор Google Абэ Гонга. В течение нескольких месяцев группа анализировала алгоритмы, выработанные нейронными сетями, и сравнивала их с массивами статистических данных о преступности. В сентябре 2016 г. группа вынесла решение, с которым согласились и создатели COMPAS, и экспертное сообщество Propublica. Абэ Гонг подтвердил, что алгоритмы COMPAS по построению нейронных сетей и глубокому обучению математически безупречны, как и сама программа в статистическом смысле. Статистическая безупречность означает, что нейронным сетям удалось установить наиболее точную зависимость между выходными данными и входными, т. е. между данными, представляющими профиль того или иного индивида, и критериями риска.

Все рекомендации COMPAS были верны в инженерном смысле этого слова: программа действительно минимизировала число условно-досрочных освобождений, после которых нарушители закона вновь совершали преступления, а также правильно определяла, в каких случаях перспективнее было бы отпустить человека под залог.

Таким образом, общество, правоохранительная и судебная система поставлены искусственным интеллектом перед серьезной морально-этической дилеммой, пути выхода из которой пока не обозначены. Не менее важные задачи ставятся в поисках возможностей искусственного интеллекта в предупреждении преступности (табл. 4).

В докладе SOCTA (Serious and Organized Crime Threat Assessment)[3] говорится о том, что

[3] Доклад «Оценка угрозы со стороны особо опасных

Таблица 4 / Table 4

Искусственный интеллект в предупреждении преступности
Artificial intelligence in preventing crime

Наименование программы (эксперимента) / Name of the program (experiment)	Сфера применения / Sphere of use
Интегрированная геолокационная платформа предиктивной аналитики (Манчестер, Великобритания, 2016 г. — н. в.)	Профилактика уличной преступности за счет повышенного внимания полиции к улице или участку улицы при изменении факторов, воздействующих на уровень данного вида преступности [19, с. 168–169]
Система анализа данных, основанная на разработках IBM и географической информационной системе Ersi (Ванкувер, Канада, 2007 г. — н. в.)	Выявление тенденций преступности, прогнозирование вероятного времени и места совершения преступления. С 2007 по 2011 г. количество преступлений, связанных с собственностью, сократилось на 24 %, уровень насильственной преступности — на 9 % [там же, с. 44–45]
Эксперимент, направленный на профилактику индивидуальной преступности рецидивистов (Квебек, Канада, 2015 г. — н. в.)	Находящимся в заключении рецидивистам с учетом тяжести их преступлений предлагается условно-досрочное освобождение в обмен на согласие разместить на своем теле татуировку, представляющую собой сверхтонкий процессор-индикатор, который меняется раз в пять лет [4, с. 171–172]

Окончание табл. 4 / End of the table 4

Наименование программы (эксперимента) / Name of the program (experiment)	Сфера применения / Sphere of use
Программа по созданию системы социального кредита (КНР, 2014–2020 гг.).	К 2020 г. планируется отслеживать и оценивать в режиме реального времени каждого жителя материкового Китая. Рейтинг доверия физических лиц привязывается к социальному паспорту. Обладатели высокого рейтинга пользуются различными социальными и экономическими льготами, обладатели низкого рейтинга подпадают под административные санкции и ограничения. Система уже работает в пилотном режиме в 30 городах Китая. Жителям дается стартовый рейтинг в 1 тыс. баллов и далее в зависимости от их поведения либо растет, либо падает. Единый информационный центр анализирует 160 тыс. различных параметров из 142 учреждений. Приветствуется система доносов (донос повышает рейтинг на пять баллов)* [4, с. 193–198]

* Planning Outline for the Construction of a Social Credit System (2014–2020). URL: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020.

важнейшей задачей при создании прогностико-мониторинговых систем является разработка и проверка статистически обоснованной системы индикаторов раннего предупреждения преступности (EWS). К ним относятся:

– *показатели совпадения* — индикаторы, которые имеют высокую степень корреляции и (или) однонаправленную динамику;

– *запаздывающие индикаторы* — показатели, которые формируются после тех или иных изменений в изучаемом объекте;

– *циклические индикаторы* — показатели, которые с различной степенью опережения либо без нее характеризуют переход наблюдаемой системы из одной циклической фазы в другую;

– *контрциклические индикаторы* — показатели, улавливающие разнонаправленность системной динамики [4, с. 291–293].

Повсеместное внедрение и совершенствование информационных технологий побуждают и нашу страну принимать соответствующие правовые и управленческие решения, направленные на то, чтобы упорядочить эту сферу и обозначить вектор ее развития.

В 2013 г. была разработана «дорожная карта» развития информационных технологий[4]; в 2014 г. принята государственная программа Российской Федерации «Информационное общество (2011–2020 годы)»[5]; указом Президента РФ утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[6]; реализуются мероприятия программы «Цифровая экономика Российской Федерации»[7]. Основные направления обеспечения информационной безопасности в области государственной и общественной безопасности определены Доктриной информационной безопасности Российской Федерации, утвержденной указом Президента РФ от 5 декабря 2016 г. № 646[8].

«В кратчайшие сроки нам необходимо создать передовую законодательную базу, снять все барьеры для разработки и широкого применения робототехники, искусственного интеллекта, беспилотного транспорта, электронной торговли, технологий обработки больших данных. Причем такая нормативная база должна постоянно обновляться, строиться на гибком подходе к каждой сфере и технологии», — заявил Пре-

форм организованной преступности» разрабатывается и публикуется Европолом в сотрудничестве с консультативной группой SOCTA, в состав которой входят государства — члены ЕС, агентства ЕС, Европейская комиссия и Генеральный секретариат Совета при поддержке европейских стран-партнеров и организаций Европола.

[4] Об утверждении плана мероприятий («дорожной карты») «Развитие отрасли информационных технологий» : распоряжение Правительства РФ от 30 дек. 2013 г. № 2602-р : (ред. от 5 дек. 2014 г.). URL: http://base.garant.ru/70555876.

[5] Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» : постановление Правительства РФ от 15 апр. 2014 г. № 313 : (ред. от 12 авг. 2017 г.) // Собрание законодательства РФ. 2014. № 18, ч. 2. Ст. 2159.

[6] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // Там же. 2017. № 20. Ст. 2901.

[7] Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р // Там же. № 32. Ст. 5138.

[8] Собрание законодательства РФ. 2016. № 50. Ст. 7074.

зидент Российской Федерации 1 марта 2018 г., обращаясь к Федеральному Собранию[9].

В отраслевых документах обозначается значимость повышения эффективности противодействия *преступности, использующей информационные технологии,* но стратегическая задача применения информационных технологий *в прогнозировании и предупреждении* преступности не выдвигается.

В государственной программе «Обеспечение общественного порядка и противодействие преступности» предусмотрено «внедрение в служебную деятельность новых информационных технологий», однако можно предположить, что речь идет преимущественно о технологиях, направленных на фиксацию и раскрытие преступлений[10]. В сфере использования возможностей искусственного интеллекта в противостоянии преступности, и особенно в сфере профилактики, наша страна, увы, находится далеко не на передовых позициях.

Между тем происходящие изменения, обусловленные развитием цифровых технологий, отличаются такой характеристикой, как *стремительность*. В 2011 г. на Ганноверской выставке была изложена концепция четвертой промышленной революции («Индустрии 4.0»), которая, по мнению участников мероприятия, должна была привести к слиянию технологий и размыть границы между физической, цифровой и биологической сферами, а спустя совсем непродолжительное время под эгидой японской федерации крупного бизнеса «Кэйданрэн» были разработаны основы программы создания суперинтеллектуального общества, или «Общества 5.0». Стратегия «Общества 5.0» не ограничена только производственным сектором, она призвана решать социальные проблемы с помощью интеграции физического и киберпространства. «Кэйданрэн» объявляет, что «Общество 5.0» — это социально-экономическая и культурная система, основанная на передовых цифровых технологиях (большие данные, искусственный интеллект, дополненная реальность), с одной стороны, и обеспечивающая развитие науки и технологий на благо каждого члена общества, с другой стороны.

Старший генеральный менеджер подразделения внешних и правительственных связей корпорации Mitsubishi Electric Норицугу Уэмура обозначил «пять стен», которые, по его мнению, необходимо преодолеть для развития цифровой экономики. Первая из этих стен — стена министерств и ведомств, поскольку для движения вперед нужна четкая национальная стратегия и поддержка инициатив государством вплоть до создания новых органов власти. Вторая стена — законодательная система: на примере многих стран видно, как прогресс буксует, упираясь в устаревшие законодательные нормы. Третья стена — технологии (необходимо формирование базы знаний, чтобы каждый мог воспользоваться преимуществами цифровой экономики). Четвертая стена — человеческие ресурсы: требуется объяснять людям, как работает цифровая экономика, и обучать их, чтобы они были готовы творить. И, наконец, пятая стена — принятие обществом. «Если эти пять стен удастся преодолеть, плоды «Общества 5.0» сможет потреблять не только Япония, но и весь остальной мир. Ведь цифровая экономика во многом стирает физические границы», — пишет Н. Уэмура [33].

Полагаем, что обозначенные пять стен имеют быть и в сфере повсеместного внедрения искусственного интеллекта в систему противодействия преступности в нашей стране. Концепция пяти стен, которые нужно как можно скорее ликвидировать, может быть положена в основу Современной стратегии противодействия преступности, ее прогнозирования и предупреждения в Российской Федерации. Констатация отставания России в этой области диктует необходимость в кратчайшие сроки разработать «дорожную карту» внедрения технологий искусственного интеллекта в систему противодействия преступности, ее прогнозирования и предупреждения. Современная стратегия противодействия преступности, ее прогнозирования и предупреждения в Российской Федерации должна, на наш взгляд, предусматривать следующие направления:

1. Признание противодействия преступности, ее прогнозирования и предупреждения с использованием современных технологий приоритетной задачей государства наряду с развитием экономики, образования, медицины, усилением обороноспособности страны.

2. Инициирование общественной дискуссии по морально-этическим и правовым аспектам использования современных технологий в борьбе с преступностью в целях достижения

[9] Российская газета. 2018. 2 марта.

[10] Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности» : постановление Правительства РФ от 15 апр. 2014 г. № 345 : (ред. от 30 марта 2018 г.) // Собрание законодательства РФ. 2014. № 18, ч. 4. Ст. 2188.

общественного согласия относительно пределов вторжения современных программных решений в частную и частно-публичную жизнь граждан.

3. Опережающее развитие законодательной базы, исключающей наличие необоснованных правовых барьеров перед внедрением новейших технологических достижений.

4. Изучение зарубежного опыта по использованию искусственного интеллекта в сфере противодействия преступности, ее прогнозирования и профилактики, внедрение передовых технологий в деятельность российских правоохранительных органов.

5. Разработка современных моделей противодействия преступности, ее прогнозирования и предупреждения с использованием цифровых технологий и искусственного интеллекта.

6. Стимулирование разработки отечественных программных решений, направленных на противодействие преступности, ее прогнозирование и предупреждение, путем объединения возможностей государства, образовательных организаций, научных учреждений и частного бизнеса в реализации соответствующих тактических решений.

7. Создание и объединение мощных, доступных сотрудникам правоохранительных органов всех уровней баз данных, наполнение которых основано на едином стандарте технических и программных требований, повсеместное внедрение в штат специалистов в области аналитики больших данных.

8. Сплошное повышение квалификации сотрудников правоохранительных органов на курсах подготовки в области использования современных технологий.

9. Внедрение элементов профилактики виктимного поведения потенциальных жертв преступлений в информационном пространстве (в образовательных организациях всех уровней, на предприятиях, среди лиц пожилого возраста и др.).

10. Включение курсов «Цифровая криминалистика» и «Цифровая криминология» в образовательные программы подготовки специалистов уголовно-правовой специализации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Цифровая цивилизация. Россия и «электронный» мир XXI века / С. Ю. Глазьев [и др.]. — М. : Кн. мир, 2018. — 288 с.

2. Reese H. Understanding the differences between AI, machine learning, and deep learning [Electronic resource] / H. Reese. — Mode of access: https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning.

3. Боровская Е. В. Основы искусственного интеллекта / Е. В. Боровская, Н. А. Давыдова. — М. : Лаборатория знаний, 2018. — 127 с.

4. Ларина Е. С. Искусственный интеллект. Большие данные. Преступность / Е. С. Ларина, В. С. Овчинский. — М. : Кн. мир, 2018. — 416 с.

5. Aiello M. F. Policing through social networking: Testing the linkage between digital and physical police practices / M. Aiello // The Police Journal. — 2018. — Vol. 91, iss. 1. — P. 89–101. — DOI: https://doi.org/10.1177/0032258X17690932.

6. Chattoe E. It's not who you know — it's what you know about people you don't know that counts: extending the analysis of crime groups as social networks / E. Chattoe, E. Hamill // The British Journal of Criminology. — 2005. — Vol. 45, iss. 6. — P. 860–876. — DOI: 10.1093/bjc/azi051.

7. Goodison S. E. Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence [Electronic resource] / S. E. Goodison, R. C. Davis, B. A. Jackson. — Mode of access: https://www.rand.org/pubs/research_reports/RR890.html.

8. Hagen J. Protecting the Digitized Society — the Challenge of Balancing Surveillance and Privacy / J. Hagen, O. Lysne // The Cyber Defense Review. — 2016. — Vol. 1, № 1. — P. 75–90.

9. Hannah-Moffat K. Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates / K. Hannah-Moffat // Theoretical Criminology. — 2018. — DOI: 10.1177/1362480618763582.

10. Powell A. Digital Criminology: Crime and Justice in Digital Society / A. Powell, G. Stratton, R. Cameron. — London : Routledge, 2018. — 210 p.

11. Revier K. «Now You're Connected»: Carceral Visuality and Police Power on MobilePatrol / K. Revier // Theoretical Criminology. — 2018. — DOI: 10.1177/1362480618779401.

12. Wilner A. S. Cybersecurity and its Discontents: Artificial Intelligence, the Internet of Things, and Digital Misinformation / A. S. Wulner // International Journal. — 2018. — Vol. 73, iss. 2. — P. 308–316. — DOI: 10.1177/0020702018782496.

13. Wood M. A. Algorithmic Tyranny: Psycho-Pass, Science Fiction and the Criminological Imagination / M. A. Wood // Crime, Media, Culture. — 2018. — DOI: 10.1177/1741659018774609.

14. Холостов К. М. Автоматизация процедур анализа оперативной обстановки / К. М. Холостов // Труды Академии управления МВД России. — 2014. — № 1. — С. 22–26.

15. Осипенко А. Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения / А. Л. Осипенко // Вестник Воронежского института МВД России. — 2015. — № 2. — С. 13–19.

16. Яковец Е. Н. Оперативно-разыскные меры полиции по обеспечению информационной безопасности Российской Федерации / Е. Н. Яковец // Труды Академии управления МВД России. — 2017. — № 3. — С. 127–131.

17. Кравцов Д. А. Искусственный разум: предупреждение и прогнозирование преступности / Д. А. Кравцов // Вестник Московского университета МВД России. — 2018. — № 3. — С. 108–110.

18. Овчинский В. С. Мафия: новые мировые тенденции / В. С. Овчинский. — М. : Кн. мир, 2016. — 384 с.

19. Овчинский В. С. Технологии будущего против криминала / В. С. Овчинский. — М. : Кн. мир, 2017. — 288 с.

20. Овчинский В. С. Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего / В. С. Овчинский. — М. : Кн. мир, 2018. — 320 с.

21. Ларина Е. С. Криминал будущего уже здесь / Е. С. Ларина, В. С. Овчинский. — М. : Кн. мир, 2018. — 512 с.

22. Овчинский В. С. Криминология цифрового мира : учеб. для магистратуры / В. С. Овчинский. — М. : Норма, 2018. — 352 с.

23. Ларина Е. С. Роботы-убийцы против человечества. Кибер-апокалипсис сегодня / Е. С. Ларина, В. С. Овчинский. — М. : Кн. мир, 2018. — 416 с.

24. Когалов Ю. Покушение на Мадуро готовили полгода / Ю. Когалов // Российская газета. — 2018. — 6 авг.

25. Ефремова Э. Искусственный интеллект научился делать фейковые видео [Электронный ресурс] / Э. Ефремова. — Режим доступа: https://www.ridus.ru/news/266977.

26. Ализар А. Нейросеть сделала фальшивого Обаму [Электронный ресурс] / А. Ализар. — Режим доступа: https://habr.com/post/405269.

27. Ламинина О. Г. Возможности социальной инженерии в информационных технологиях / О. Г. Ламинина // Гуманитарные, социально-экономические и общественные науки. — 2017. — № 2. — С. 21–23.

28. Mann I. Hacking the Human / I. Mann. — London : Routledge, 2017. — 266 p.

29. Мурсалиева Г. Видите призыв к суициду — срочно жмите на кнопку «Пожаловаться» / Г. Мурсалиева // Новая газета. — 2017. — 6 марта.

30. Филатов А. «Известия» нашли автора бота, заманивающего детей в «группы смерти» / А. Филатов // Известия. — 2017. — 11 авг.

31. Ильченко С. Предлагать интим. Как роботы разводят людей на секс и деньги [Электронный ресурс] / С. Ильченко. — Режим доступа: http://www.dsnews.ua/society/potolkuem-malost-kogda-boty-nachnut-upravlyat-lyudmi-20072017220000.

32. Евдокимов К. Н. Анекселенктотичная технотронная преступность (частная теория) / К. Н. Евдокимов // Российский судья. — 2018. — № 4. — С. 35–39.

33. Уэмура Н. Стратегия «Общество 5.0» / Н. Уэмура // Известия. — 2017. — 13 марта.

REFERENCES

1. Glazev S. Yu., Ovchinskii V. S., Larina E. S., Kalashnikov M., Nagornyi A. A. *Tsifrovaya tsivilizatsiya. Rossiya i «elektronnyi» mir XXI veka* [Digital civilization. Russia and the «electronic» world of the 21st century]. Moscow, Knizhnyi Mir Publ., 2018. 288 p.

2. Reese H. *Understanding the differences between AI, machine learning, and deep learning*. Available at: https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning.

3. Borovskaya E. V., Davydova N. A. *Osnovy iskusstvennogo intellekta* [Basics of Artificial Intelligence]. Moscow, Laboratoriya Znanii Publ., 2018. 127 p.

4. Larina E. S., Ovchinskii V. S. *Iskusstvennyi intellekt. Bol'shie dannye. Prestupnost'* [Artificial Intelligence. Big Data. Crime]. Moscow, Knizhnyi Mir Publ., 2018. 416 p.

5. Aiello M. F. Policing through social networking: Testing the linkage between digital and physical police practices. *The Police Journal*, 2018, vol. 91, iss. 1, pp. 89–101. DOI: https://doi.org/10.1177/0032258X17690932.

6. Chattoe E., Hamill E. It's not who you know — it's what you know about people you don't know that counts: extending the analysis of crime groups as social networks. *The British Journal of Criminology,* 2005, vol. 45, iss. 6, pp. 860–876. DOI: 10.1093/bjc/azi051.

7. Goodison S. E., Davis R. C., Jackson B. A. *Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Available at: https://www.rand.org/pubs/research_reports/RR890.html.

8. Hagen J., Lysne O. Protecting the Digitized Society — the Challenge of Balancing Surveillance and Privacy. *The Cyber Defense Review*, 2016, vol. 1, no. 1, pp. 75–90.

9. Hannah-Moffat K. Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates. *Theoretical Criminology,* 2018. DOI: 10.1177/1362480618763582.

10. Powell A., Stratton G., Cameron R. *Digital Criminology: Crime and Justice in Digital Society*. London, Routledge, 2018. 210 p.

11. Revier K. «Now You're Connected»: Carceral Visuality and Police Power on MobilePatrol. *Theoretical Criminology*, 2018. DOI: 10.1177/1362480618779401.

12. Wilner A. S. Cybersecurity and its Discontents: Artificial Intelligence, the Internet of Things, and Digital Misinformation. *International Journal*, 2018, vol. 73, iss. 2, pp. 308–316. DOI: 10.1177/0020702018782496.

13. Wood M. A. Algorithmic Tyranny: Psycho-Pass, Science Fiction and the Criminological Imagination. *Crime, Media, Culture*, 2018. DOI: 10.1177/1741659018774609.

14. Kholostov K. M. Automation of routines for operational environment analysis. *Trudy Akademii upravleniya MVD Rossii = Proceedings of the Management Academy of the Ministry of the Interior of Russia,* 2014, no. 1, pp. 22–26. (In Russian).

15. Osipenko A. L. New Technologies of Obtaining and Analyzing Operational Investigative Information: Legal Problems and Implementation Prospects. *Vestnik Voronezhskogo instituta MVD Rossii = Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2015, no. 2, pp. 13–19. (In Russian).

16. Yakovets E. N. Police Detection and Search Operations Aimed at Protecting the Information Security of the Russian Federation. *Trudy Akademii upravleniya MVD Rossii = Proceedings of the Management Academy of the Ministry of the Interior of Russia,* 2017, no. 3, pp. 127–131. (In Russian).

17. Kravtsov D. A. Artificial Intelligence: Crime Prevention and Prediction. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of Moscow University of the Ministry of Internal Affairs of Russia*, 2018, no. 3, pp. 108–110. (In Russian).

18. Ovchinskii V. S. *Mafiya: novye mirovye tendentsii* [Mafia: New Global Trends]. Moscow, Knizhnyi Mir Publ., 2016. 384 p.

19. Ovchinskii V. *Tekhnologii budushchego protiv kriminala* [Future Technologies against Crimes]. Moscow, Knizhnyi Mir Publ., 2017. 288 p.

20. Ovchinskii V. S. *Virtual'nyi shchit i mech: SShA, Velikobritaniya, Kitai v tsifrovykh voinakh budushchego* [Virtual shield and sword: the US, the UK, China in digital wars of the future]. Moscow, Knizhnyi Mir Publ., 2018. 320 p.

21. Larina E., Ovchinskii V. *Kriminal budushchego uzhe zdes'* [The Crimes of the Future are Already Here]. Moscow, Knizhnyi Mir Publ., 2018. 512 p.

22. Ovchinskii V. S. *Kriminologiya tsifrovogo mira* [Criminology of the digital world]. Moscow, Norma Publ., 2018. 352 p.

23. Larina E. S., Ovchinskii V. S. *Roboty-ubiitsy protiv chelovechestva. Kiber-apokalipsis segodnya* [Robot killers against humanity. Cyber-apocalypses today]. Moscow, Knizhnyi Mir Publ., 2018. 416 p.

24. Kogalov Yu. It took half a year to prepare Maduro's failed assassination. *Rossiiskaya Gazeta,* 2018, August 6. (In Russian).

25. Efremova E. *Iskusstvennyi intellekt nauchilsya delat' feikovye video* [Artificial intelligence has learnt to make fake videos]. Available at: https://www.ridus.ru/news/266977. (In Russian).

26. Alizar A. *Neiroset' sdelala fal'shivogo Obamu* [Neural network created a fake Obama]. Available at: https://habr.com/post/405269. (In Russian).

27. Laminina O. G. Possibilities of Social Engineering in Information Technologies. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki = Humanities, Social-Economic and Social Sciences,* 2017, no. 2, pp. 21–23. (In Russian).

28. Mann I. *Hacking the Human.* London, Routledge, 2017. 266 p.

29. Mursalieva G. You see calls to commit suicide — press «complain» button fast. *Novaya Gazeta*, 2017, March 6. (In Russian).

30. Filatov A. *Izvestiya* found the author of the bot who lured children into «death groups». *Izvestiya*, 2017, August 11. (In Russian).

31. Ilchenko S. *Predlagat' intim. Kak roboty razvodyat lyudei na seks i den'gi* [Offer sex. How robots dupe people for sex and money]. Available at: http://www.dsnews.ua/society/potolkuem-malost-kogda-boty-nachnut-upravlyat-lyudmi-20072017220000. (In Russian).

32. Evdokimov K. N. Anexelenctotic Technotronic Crime (Sub-theory). *Rossiiskii sudya = Russian Judge,* 2018, no. 4, pp. 35–39. (In Russian).

33. Uemura N. Strategy «Society 5.0». *Izvestiya*, 2017, March 13. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Суходолов Александр Петрович — ректор Байкальского государственного университета, профессор, г. Иркутск, Российская Федерация; e-mail: rector@bgu.ru.

Бычкова Анна Михайловна — член Ассоциации юристов России, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: amb-38@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Суходолов А. П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А. П. Суходолов, А. М. Бычкова // Всероссийский криминологический журнал. — 2018. — Т. 12, № 6. — С. 753–766. — DOI: 10.17150/2500-4255.2018.12(6).753–766.

INFORMATION ABOUT THE AUTHORS

Sukhodolov, Alexander P. — Rector of Baikal State University, Professor, Irkutsk, the Russian Federation; e-mail: rector@bgu.ru.

Bychkova, Anna M. — Member, Association of Russian Lawyers, Ph. D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: amb-38@mail.ru.

FOR CITATION

Sukhodolov A. P., Bychkova A. M. Artificial intelligence in crime counteraction, prediction, prevention and evolution. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 6, pp. 753–766. DOI: 10.17150/2500-4255.2018.12(6).753–766. (In Russian).