EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
IF = 9.3 www.in-academy.uz/index.php/ejar

CRIMES COMMITTED USING ARTIFICIAL INTELLIGENCE: TYPES AND PUBLIC DANGER

Muzaffar Ziyodullaevich Ziyodullayev
Doctor of Law, Professor
Tashkent International University
Tashkent, Uzbekistan
e-mail: muzzziyo@gmail.com
https://doi.org/10.5281/zenodo.19331153

ARTICLE INFO

Received: 24th March 2026
Accepted: 29th March 2026
Online: 30th March 2026

KEYWORDS

Artificial intelligence, cybercrime, deepfake, fraud, theft, dissemination of slander using artificial intelligence, extortion, production and distribution of pornographic materials, acts of a religious-extremist and terrorist nature.

ABSTRACT

Based on specific examples, this article examines current trends in the use of artificial intelligence technologies for criminal purposes, as well as the types, specific features, and public danger of crimes committed using artificial intelligence. In addition, the nature of this type of crime is revealed, and relevant conclusions are formulated to increase the effectiveness of countermeasures.

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ВИДЫ И ОБЩЕСТВЕННАЯ ОПАСНОСТЬ

Музаффар Зиёдуллаевич Зиёдуллаев
доктор юридических наук, профессор
Tashkent International University. Ташкент, Узбекистан
e-mail: muzzziyo@gmail.com
https://doi.org/10.5281/zenodo.19331153

ARTICLE INFO

Received: 24th March 2026
Accepted: 29th March 2026
Online: 30th March 2026

KEYWORDS

Искусственный интеллект, киберпреступность, дипфейк, мошенничество, кража, распространение клеветы с использованием искусственного интеллекта,

ABSTRACT

В данной статье на основе конкретных примеров исследованы современные тенденции использования технологий искусственного интеллекта в преступных целях, а также виды, специфические особенности и общественная опасность преступлений, совершаемых с использованием искусственного интеллекта. Наряду с этим, раскрывается природа преступлений данного вида и формулируются соответствующие выводы по повышению эффективности противодействия им.

вымогательство, изготовление и распространение порнографических материалов, действия религиозно-экстремистского и террористического характера.

На сегодняшний день «искусственный интеллект» стал неотъемлемой частью жизни общества. Хотя данный термин впервые был употреблен и раскрыт в 1950 году в труде английского математика Алана Тьюринга «Вычислительные машины и разум» [22], в научный оборот он был введен в 1956 году американским ученым Джоном Маккарти на Дартмутской конференции [17].

За прошедшие годы рядом ученых были даны различные определения понятию «искусственный интеллект», основанные на разных подходах. В частности, Родриго Гонсалес в своем диссертационном исследовании дает следующее определение: «искусственный интеллект связан с созданием и функционированием запрограммированных машин, причем такие машины могут выполнять и выполняют работу, которая, как считается, требует определенного уровня разума (интеллекта) и разумности» [10].

Российский ученый Л.С. Болотова определяет искусственный интеллект как «искусственную систему, способную имитировать человеческое мышление, обладающую способностью к извлечению, обработке, хранению информации и знаний, а также к выполнению над ними различных операций» [20]. Высказывая схожую точку зрения, В.Н. Ручкин и В.А. Фулин выдвигают определение, согласно которому «искусственный интеллект – это комплекс метапроцедур, имитирующих человеческую деятельность, то есть совокупность представления знаний, рассуждений, поиска соответствующей информации в среде существующих знаний, их пополнения, корректировки и тому подобного» [25]. По мнению Е.В. Соломонова, «искусственный интеллект – это автономная система, обладающая способностью принимать самостоятельные решения без участия человека, к самообучению и решению сложных задач» [26].

По мнению П.Г. Уинстона, важнейшие задачи разработки и внедрения искусственного интеллекта заключаются в понимании принципов, лежащих в основе естественного интеллекта, и изучении их применения в технике и технологиях, а также в повышении полезности вычислительных машин и

привлечении их к решению сложных проблем [27]. С.Дж. Рассел, в свою очередь, приходит к выводу, что «традиционные цели исследований искусственного интеллекта включают в себя рассуждение, представление знаний, планирование, обучение, обработку естественного языка, восприятие и поддержку робототехники» [15].

Впервые в нашей стране Законом Республики Узбекистан от 21 января 2026 года № ЗРУ-1115 «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с урегулированием отношений, возникающих при применении искусственного интеллекта» в Закон «Об информатизации» было введено правовое определение понятия «искусственный интеллект»: «*искусственный интеллект* – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (в том числе самообучение и поиск решений) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека» [1].

В XX веке философ Джон Сёрл, рассуждая об искусственном интеллекте, разделил его на сильный и слабый: «Сильный искусственный интеллект способен осознавать себя и мыслить как человек, он обладает сознанием, эмоциями, мышлением и, не ограничиваясь одной конкретной сферой, способен принимать решения в нескольких областях. Слабый же искусственный интеллект не обладает такими способностями, он решает узкоспециализированные задачи (например, в сфере программного обеспечения беспилотных транспортных средств)» [16].

В качестве основных юридически значимых признаков искусственного интеллекта можно выделить следующие:

автономность – способность действовать без контроля со стороны человека;

самообучение – способность системы автоматически совершенствовать собственные алгоритмы с опорой на накопленные данные и практический опыт;

прогнозирование – способность предвидеть будущие ситуации на основе анализа больших массивов данных (Big Data).

На современном этапе развитие информационно-телекоммуникационных технологий, наряду с созданием возможностей для прогресса во всех сферах жизнедеятельности общества, порождает и новые факторы, оказывающие негативное влияние на криминогенную обстановку. Системы искусственного интеллекта стремительно внедряются не только в экономическую и социальную сферы, но и в преступную деятельность криминальных группировок и отдельных правонарушителей. На сегодняшний день темпы роста преступлений, совершаемых с использованием искусственного интеллекта, продолжают оставаться высокими в мировом масштабе. Данная категория деяний в корне

отличается от традиционных видов преступлений своим высоким технологическим уровнем, дистанционным характером и анонимностью.

Возникает закономерный вопрос: какие именно преступления совершаются на сегодняшний день с использованием искусственного интеллекта и каковы их специфические особенности, отграничивающие их от иных преступных деяний?

Исследования и анализ показывают, что злоумышленники могут использовать возможности искусственного интеллекта при совершении следующих преступлений:

Мошенничество. На сегодняшний день киберпреступники активно используют различные виды вредоносного программного обеспечения для совершения противоправных действий в онлайн-среде: *вирусы* – проникают в систему, размножаются и повреждают файлы и программы, позволяя использовать их в целях хищения персональных данных и финансового мошенничества; *троянские программы* – маскируются под легитимное (полезное) программное обеспечение, однако в действительности скрывают вредоносные функции, предоставляя возможность удаленного доступа к компьютеру, сбора конфиденциальной информации и совершения вымогательства; *шпионские программы* – устанавливаются незаметно для пользователя, позволяя осуществлять сбор информации о действиях в сети, а также отслеживать пароли, банковские реквизиты и иные критически важные данные; *программы-вымогатели (ransomware)* – используются для шифрования файлов на компьютере с последующим требованием выкупа за их восстановление (дешифровку).

Кибермошенничество с использованием искусственного интеллекта охватывает следующие технологии:

создание поддельного контента – искусственный интеллект применяется для генерации фейковых изображений, видео или текстов с высокой степенью реалистичности, что позволяет мошенникам создавать дезинформирующие материалы с целью обмана и манипулирования целевой аудиторией;

автоматизированные атаки на пароли и системы безопасности – искусственный интеллект может применяться для разработки и оптимизации методов взлома паролей и обхода систем безопасности за относительно короткий промежуток времени;

социальная инженерия – искусственный интеллект используется для анализа данных о потенциальных жертвах и генерации персонализированных мошеннических сообщений, что позволяет проводить гораздо более успешные фишинговые кампании по обману пользователей и завладению их конфиденциальной информацией [24].

Кроме того, на практике искусственный интеллект может

использоваться в следующих видах кибермошеннических операций: *бот-мошеннические атаки на базе искусственного интеллекта*, отличающиеся способностью обрабатывать текстовые сообщения и с высокой точностью имитировать человеческий голос, при этом данные технологии направлены на полную автоматизацию процессов финансового мошенничества и дистанционное завладение персональными данными жертвы; *создание алгоритмов с помощью искусственного интеллекта для обмана* торговых платформ или автоматической генерации фиктивных транзакций; генерация фейковых новостей с использованием искусственного интеллекта для их распространения в социальных сетях с целью введения в заблуждение общественного мнения или провоцирования паники среди населения [23].

Старший советник Лондонской фондовой биржи (LSEG) Рут Вандхёфер, рассуждая о новой эре угроз автономного искусственного интеллекта, отмечает, что в последнее время хакеры осваивают искусственный интеллект быстрее, чем бизнес. Она подчеркивает, что количество атак с использованием программ-вымогателей (ransomware, то есть блокирование данных пользователя или всей компьютерной системы с требованием выкупа за их восстановление) возросло на 60%, среди пострадавших числятся крупные бренды, банки и даже крупные оборонные организации, а злоумышленники начали массово использовать искусственный интеллект для автоматизации фишинга и создания дипфейков. По ее мнению, обеспокоенность в этой сфере усиливают следующие факторы: появление систем, способных самостоятельно выполнять сложные операции без вмешательства человека; снижение надежности традиционных методов аутентификации личности; неосознанная передача сотрудниками конфиденциальных корпоративных данных в публично доступные алгоритмы; рост киберпреступлений в формате Onchain, то есть случаев, когда преступники все чаще атакуют платформы DeFi (систему децентрализованных банковских и финансовых услуг, функционирующих без участия банков или государства и централизованного управления) и переносят свою инфраструктуру в блокчейн во избежание ответственности; стремление к созданию квантовых компьютеров, способных взламывать классическое шифрование [18].

Кража. С использованием искусственного интеллекта могут совершаться следующие виды краж:

Совершение кражи путем имитации голоса (Deepfake audio) или подделки внешности (Deepfake) лица – проявляется в том, что с помощью искусственного интеллекта подделывается голос или внешность руководителя либо близкого человека, и по телефону или видеосвязи дается указание о переводе денежных средств. Также это выражается в совершении кражи с

проникновением в жилище или иной объект путем обмана современных систем безопасности за счет подделки биометрических данных (внешности).

Первая кража, совершенная с использованием голосового дипфейка, сгенерированного искусственным интеллектом, была зафиксирована в Великобритании. В данном случае генеральный директор неназванной энергетической компании, полагая, что разговаривает по телефону со своим руководителем – главным исполнительным директором материнской компании в Германии, немедленно выполнил указание о переводе средств в размере 220 тысяч евро (около 243 тысяч долларов США) на банковский счет венгерского поставщика [3].

За прошедшие годы по всему миру был совершен ряд подобных краж. В частности, в начале 2020 года руководителю филиала японской компании в Гонконге позвонили от имени генерального директора компании и попросили подтвердить денежные переводы на сумму 35 млн долларов США в связи с процессом приобретения компании. Поскольку электронные письма и другие данные также выглядели достоверными, руководитель осуществил денежные переводы. Позже выяснилось, что это была сложная схема киберхищения, реализованная путем клонирования голоса директора с помощью технологии «deep voice» на базе искусственного интеллекта. По данным Forbes, в этом преступлении участвовало не менее 17 человек, а похищенные средства были переведены на банковские счета в разных странах [9].

Также в 2024 году в Гонконге злоумышленники, используя технологию дипфейк на базе искусственного интеллекта, в ходе видеоконференции продемонстрировали сотруднику международной компании искусственно сгенерированные образы главного финансового директора и других сотрудников компании, по указанию которых он перевел на различные банковские счета 200 млн гонконгских долларов (около 25–26 млн долларов США) [8].

В Узбекистане также изо дня в день растет число киберпреступлений, количество их видов увеличилось с 18 до 62. В особенности набирают обороты кража персональных данных, имитация голоса и внешности с помощью искусственного интеллекта, распространение вредоносных файлов. За последние шесть лет количество обращений по фактам киберпреступлений в нашей стране возросло в 48 раз. В прошлом году 82 процента совершенных мошенничеств и 76 процентов краж были осуществлены в киберпространстве. Нанесенный ими материальный ущерб физическим и юридическим лицам превысил 2 триллиона сумов. Присвоенные средства выводятся за рубеж в виде криптовалюты. Особое сожаление вызывает тот факт, что 95 процентов синтетических наркотиков распространяются через интернет, а оплата за них производится в криптовалюте [2].

Автоматизированное хищение средств с банковских счетов – системы искусственного интеллекта путем анализа алгоритмов банковской безопасности осуществляют транзакции под видом естественных операций, что позволяет обходить системы антифрода (antifraud). Согласно отчету Лаборатории Касперского, киберпреступники используют ботов на базе искусственного интеллекта, которые автоматически собирают финансовые данные и осуществляют транзакции [13].

Искусственный интеллект, анализируя данные социальных сетей, позволяет создавать сценарии краж на основе социальной инженерии и коды для кибератак. Согласно отчету Европола, возможности генеративных моделей, таких как ChatGPT, по написанию кода со временем развиваются. Новейшие генеративные модели обладают способностью лучше понимать контекст кода, выявлять ошибки и устранять недостатки программирования. Это может позволить лицам, не обладающим техническими знаниями, создавать инструменты для киберпреступлений, а опытным пользователям – совершенствовать или автоматизировать сложные методы совершения киберпреступлений [6].

Использование искусственного интеллекта при краже криптоактивов – выражается в том, что преступники с помощью технологий искусственного интеллекта выявляют уязвимости в криптокошельках и блокчейн-системах, разрабатывают вредоносные скрипты на основе смарт-контрактов, предназначенные для их эксплуатации, и автоматизированно присваивают криптоактивы. Следовательно, хотя в последние годы в динамике преступлений, связанных с криптовалютой, в результате снижения объемов мошенничества и похищенных средств общее количество незаконных операций сократилось, тенденция к росту атак с использованием программ-вымогателей, связанных с шифрованием файлов или компьютерной системы пользователя с требованием выкупа за восстановление доступа к ним, а также активности на рынках Даркнета, сохраняется [5].

Преступления, связанные с распространением клеветы, вымогательством, изготовлением и распространением порнографических материалов, совершаемые с использованием технологий дипфейк (Deepfake) на базе искусственного интеллекта. В данных случаях преступники с помощью искусственного интеллекта могут наносить ущерб чести и достоинству личности путем использования ее образа в откровенных поддельных порнографических фото- и видеоматериалах, заниматься вымогательством под угрозой распространения фейковых порнографических материалов, а также манипулировать

общественным мнением посредством распространения сфабрикованных заявлений от имени политиков или государственных деятелей. Например, в 2024 году в социальных сетях получили широкое распространение и собрали миллионы просмотров сгенерированные искусственным интеллектом фейковые порнографические изображения известной певицы Тейлор Свифт. В результате данный инцидент обсуждался на уровне Белого дома США и ускорил продвижение законодательных инициатив по признанию дипфейк-порнографии преступлением на федеральном уровне [7].

Некоторые ученые также подчеркивают, что технологии дипфейк на базе искусственного интеллекта могут представлять определенную угрозу даже для избирательных процессов [14].

При планировании и осуществлении ***действий религиозно-экстремистского и террористического характера*** преступные группировки стремятся активно использовать возможности искусственного интеллекта, применяя его в целях расширения пропагандистской деятельности и повышения эффективности атак. В качестве основных направлений в этой сфере можно выделить следующие:

– экстремистские группировки с помощью искусственного интеллекта применяют цифровую пропаганду и технологии «Deepfake», подделывая внешность и голоса религиозных деятелей или политиков, создают фейковые проповеди и используют их для введения молодежи в заблуждение и вовлечения в радикальные идеи. Следовательно, в последние годы правоохранительными органами выявляются факты создания террористическими группировками с помощью искусственного интеллекта собственных «виртуальных проповедников», через которых ведется пропаганда на многих языках [6];

– радикализация через автоматизированные «бот-сети», при которой алгоритмы искусственного интеллекта анализируют психологические особенности пользователей социальных сетей, выявляют лиц, склонных к депрессии или подверженных влиянию, и пытаются воздействовать на них путем таргетированного распространения информации экстремистского содержания. По данным ООН, террористические группировки используют подобные технологии в целях распространения пропаганды, вербовки новых сторонников, радикализации, финансирования и координации террористических актов [12];

– террористические группировки, используя дроны, управляемые искусственным интеллектом, предпринимают попытки создания и использования систем, способных автоматически распознавать цель и осуществлять атаку без участия человека.

Еще одну категорию преступлений, совершаемых под

воздействием искусственного интеллекта, составляют **деяния, связанные с неосторожным (неумышленным) противоправным воздействием на человека и окружающую среду, либо преступления, совершаемые вследствие ошибок, допущенных разработчиками, или сбоев в процессе работы системы**. В качестве примеров можно привести дорожно-транспортные происшествия, связанные с управлением транспортными средствами и организацией дорожного движения, а также тяжкие последствия, наступившие в результате ошибок при диагностировании заболеваний и назначении лекарственных препаратов. Например, в 2018 году в США во время испытаний беспилотный автомобиль из-за сбоя в программе искусственного интеллекта насмерть сбил женщину [19]. Или же другой случай: малолетний ребенок, поступивший в больницу, скончался в результате лечения, основанного на диагнозе «грипп» и назначенных препаратах, которые были определены с помощью искусственного интеллекта. Впоследствии было установлено, что причиной смерти стала тяжелая бактериальная инфекция [11].

На сегодняшний день эффективное использование преступными группировками возможностей искусственного интеллекта при создании вредоносных кодов и автоматизации кибератак приводит к выходу угроз информационной безопасности на качественно новый уровень. Как отмечается в исследовании «Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий», проведенном ведущими американскими экспертами и учеными в области искусственного интеллекта и кибербезопасности, такими как М. Брандиж, Ш. Авин, Дж. Кларк, Х. Тонер, П. Экерсли, киберугрозам с участием искусственного интеллекта присущи следующие специфические особенности: *во-первых*, эффективность атак, то есть возможность причинения большего ущерба при меньших затратах ресурсов за счет автоматизации; *во-вторых*, наличие технологий дезинформации и дипфейка (замены или подделки внешности либо голоса человека с помощью искусственного интеллекта), в частности, способность искусственного интеллекта служить инструментом для введения в заблуждение общественного мнения и обмана людей путем изменения видео до степени, неотличимой от реальности; *в-третьих*, сложность контроля [4].

Особо следует отметить, что искусственный интеллект используется не только преступниками для совершения преступлений, но и правоохранительными органами – для эффективного противодействия преступности, обеспечения общественной безопасности и профилактики правонарушений. Роль искусственного интеллекта как

эффективного инструмента в этой сфере проявляется в следующем: он идентифицирует личность; проверяет подлинность (осуществляет аутентификацию) пользователя компьютера или электронного письма; выявляет преступные действия в электронных системах безопасности; определяет наличие оружия у субъекта; осуществляет поиск местонахождения лиц, скрывшихся после совершения преступления; выдвигает следственные версии и предлагает направления их проверки; моделирует события преступления; выявляет преступления серийного характера; содействует в проведении специальных исследований; осуществляет поиск скрытых компьютерных файлов; устанавливает первоисточник в сетях; оценивает собранные доказательства; прогнозирует оперативную обстановку и совершение преступлений на территории; анализирует деятельность организованных преступных групп, в том числе экстремистских; вычисляет каналы незаконной поставки предметов, ограниченных в обороте; прогнозирует незаконную миграцию и этническую преступность; составляет психологические портреты преступников; прогнозирует место, время и обстоятельства возможного совершения преступления конкретными лицами; выявляет ложные и противоречивые сведения в показаниях допрашиваемых лиц; отслеживает интернет-трафик и контакты фигурантов; расшифровывает коды и шифры преступников; анализирует оперативную обстановку в городах; обрабатывает изображения с камер в целях розыска правонарушителей; осуществляет биометрическую идентификацию лиц; распознает государственные номера автомобилей; извлекает необходимую информацию из мобильных телефонов; находит разыскиваемых лиц через социальные сети; определяет в городе места с высоким криминогенным риском; реализует комплексные антитеррористические меры на территориях с активизировавшейся террористической деятельностью и др. Например, в Facebook разработаны алгоритмы, которые выявляют и удаляют экстремистские посты в течение часа после их публикации, при этом искусственный интеллект распознает и удаляет 99 процентов постов, относящихся к «Исламскому государству» и «Аль-Каиде», а также 83 процента копий данных публикаций [21].

На основании вышеизложенного можно сделать следующие основные выводы:

Во-первых, современные IT-технологии и искусственный интеллект приводят к «интеллектуализации» и трансформации преступности. Искусственный интеллект в корне меняет природу традиционных преступлений (кража, мошенничество, клевета), выводя их на новый технологический уровень. Преступления, совершаемые с

использованием искусственного интеллекта, резко повышают вероятность успешного исхода кибератак не только за счет высокой точности (например, имитации голоса и внешности), но и благодаря своей способности обходить человеческий фактор и автоматизировать процессы нападения.

Во-вторых, социальная инженерия и фишинговые атаки с использованием искусственного интеллекта совершенствуются до такой степени, что обману поддаются даже опытные специалисты (о чем свидетельствуют, например, инциденты в Гонконге и Великобритании). Это означает, что в данной сфере одной лишь технической защиты недостаточно; основным направлением противодействия должно стать повышение культуры кибергигиены в обществе, осведомленности населения о рисках искусственного интеллекта, а также регулярное повышение технологической квалификации сотрудников правоохранительных органов.

В-третьих, технологии «дипфейк» (deepfake) и генеративные модели становятся орудием не только причинения финансового ущерба, но и манипулирования общественным мнением, клеветы на политических деятелей и вмешательства в избирательные процессы. Использование экстремистскими и террористическими группировками искусственного интеллекта для создания «виртуальных проповедников» или целенаправленной радикализации лиц, находящихся в депрессивном состоянии, порождает новые, еще более сложные угрозы национальной безопасности.

В-четвертых, тяжкие последствия, возникающие из-за ошибок систем искусственного интеллекта (неправильный медицинский диагноз, аварии с участием беспилотных автомобилей, необоснованные аресты вследствие сбоев в распознавании лиц и т.д.), остро ставят на повестку дня вопрос юридической ответственности. Современная правовая система пока не способна дать исчерпывающий ответ на вопрос «кто несет ответственность за ошибку искусственного интеллекта?». В связи с этим актуальнейшей задачей является правильная уголовно-правовая квалификация преступлений, связанных с искусственным интеллектом, и законодательное закрепление соответствующих этических норм.

В-пятых, искусственный интеллект представляет собой «обоюдоострое оружие»: с одной стороны, преступники используют его как орудие нападения, а с другой – для правоохранительных органов он становится наиболее эффективным инструментом в раскрытии и профилактике преступлений (распознавание лиц, прогнозирование криминогенной ситуации, киберпатрулирование). Залогом успешной борьбы в этом направлении является обеспечение того, чтобы технологические возможности и потенциал

государственных органов всегда были на шаг впереди возможностей преступного мира.

References:

1. Закон Республики Узбекистан от 21 января 2026 года № ЗРУ-1115 «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с урегулированием отношений, возникающих при применении искусственного интеллекта» // Национальная база данных законодательства. – 2026. – № 03/26/1115/0063.
2. Критически рассмотрена деятельность органов правопорядка, определены новые задачи по обеспечению общественной безопасности // [Электронный ресурс] URL: https://president.uz/ru/lists/view/8882; Борьба с организованной преступностью и киберпреступностью будет усилена // [Электронный ресурс] URL: https://president.uz/ru/lists/view/9009 (дата обращения: 15.03.2026).
3. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 // [Электронный ресурс] URL: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/ (дата обращения: 6.03.2026).
4. Brundage M., Avin S., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. – Oxford: Future of Humanity Institute, 2018. – 101 p.
5. Chainalysis: The State of Crypto Crime // [Электронный ресурс] URL: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата обращения: 6.03.2026).
6. Europol. ChatGPT – The impact of Large Language Models on Law Enforcement: A Tech Watch Flash Report from the Europol Innovation Lab. – Luxembourg: Publications Office of the European Union, 2023. – 14 p.
7. Explicit Deepfake Images of Taylor Swift Elude Safeguards and Swamp Social Media // [Электронный ресурс] URL: https://www.nytimes.com/2024/01/26/arts/music/taylor-swift-ai-fake-images.html/ (дата обращения: 8.03.2026).
8. Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’ // [Электронный ресурс] URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk (дата обращения: 6.03.2026).
9. Fraudsters Cloned Company Director’s Voice In $35 Million Heist, Police Find // [Электронный ресурс] URL: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/(дата обращения: 6.03.2026).
10. González R. The Chinese Room Revisited: Artificial Intelligence and the Nature of Mind / Dissertation presented to fulfil the requirements for the degree of Doctor in Philosophy (Ph.D.), Katholieke Universiteit Leuven // https://

lirias.kuleuven.be/bitstream/1979/939/5/The+Chinese+Room+Revisited+Artificial+Intelligence+and+the+Nature+of+Mind.pdf. – 2007. – 328 p. – P. 11.
11. Hallevy G. When Robots Kill: Artificial Intelligence Under Criminal Law. – Boston: Northeastern University Press, 2013. – p.84.
12. Information and communications technologies // [Электронный ресурс] URL: https://www.un.org/securitycouncil/ctc/content/information-and-communications-technologies (дата обращения: 8.03.2026).
13. Kaspersky: AI in Cyberattacks // [Электронный ресурс] URL: https://securelist.com/ai-and-machine-learning-in-cybercrime/108316/ (дата обращения: 6.03.2026).
14. Martin C. Deepfakes are here and can be dangerous, but ignore the alarmists – they won't harm our elections // The Guardian. – 2024. – 11 June // [Электронный ресурс] URL: https://www.theguardian.com/commentisfree/article/2024/jun/11/deepfakes-ignore-alarmists-elections (дата обращения: 8.03.2026).
15. Russell S.J. Artificial Intelligence: A Modern Approach / Stuart J. Russell, Peter Norvig. — 4th. — Hoboken: Pearson, 2021. – C. 19-26.
16. Siau K., Yang Y. Impact of artificial intelligence, robotics, and machine learning on sales and marketing // Twelve Annual Midwest Association for Information Systems Conference (MWAIS 2017) // [Электронный ресурс] URL: https://aisel.aisnet.org (дата обращения: 03.03.2026).
17. Smith C. Introduction // The History of Artificial Intelligence. – Seattle (WA, USA): University of Washington, 2006. – pp. 4.
18. Wandhöfer R. Top cyber threats and prevention trends in 2026 // [Электронный ресурс] URL: https://www.finextra.com/the-long-read/1507/top-cyber-threats-and-prevention-trends-in-2026 (дата обращения: 19.02.2026).
19. Баршев В. Раскрыта тайна смертельного наезда беспилотника Uber // [Электронный ресурс] URL://https://rg.ru/2019/11/10. (дата обращения: 8.03.2026).
20. Болотова Л.С. Системы искусственного интеллекта: модели и технологии, основанные на знаниях: учебник. – М.: Финансы и статистика, 2012. – С.28.
21. Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информазионно-телекоммуниказионных сетей, так и борьбы с ними // Вестник Московского университета МВД России. – 2022. – № 1. – С.60-65.
22. Искусственный интеллект в исследованиях сознания и общественной жизни к 70-летию статьи А. Тьюринга. «Вычислительные машины и разум» // Философия науки и техники. – 2022. – Т.27. – № 1. – С.5-6.
23. Офизиальный канал «Вестник киберполизии России» // [Электронный ресурс] URL: https://t.me/cyberpolice_rus (дата обращения: 6.03.2026).
24. Пикалов П.А. Кибермошенничество с использованием искусственного интеллекта // Актуальные вопросы борьбы с преступлениями. – 2024. – № 2. – С. 56–59.

25. Ручкин В.Н., Фулин В.А. Универсальный искусственный интеллект и экспертные системы. – СПб.: БХВ-Петербург, 2009. – С.27.
26. Соломонов Е.В. Понятие и признаки искусственного интеллекта // Вестник Омского университета. Серия «Право». – 2023. – № 4. – С.57–65.
27. Уинстон П.Г. Искусственный интеллект: Пер. с англ. В.Л. Стефанюка; под ред. Д.А. Поспелова. – М.: Мир, 1980. – С. 11