ИСПОЛЬЗОВАНИЕ ИИ В КАЧЕСТВЕ ОРУДИЯ ПРЕСТУПЛЕНИЯ

Ибрагимова Гоззал Маратовна
Инспектор группы кадрового обеспечения
Управления по координации деятельности
Органов внутренних дел Мирзо
Улугбекского района

В последние десятилетия искусственный интеллект стал одним из самых значимых и стремительно развивающихся направлений науки и технологий. Его применение охватывает практически все сферы человеческой деятельности – от медицины и промышленности до финансов и образования. ИИ позволяет автоматизировать сложные процессы, обрабатывать огромные объемы данных, принимать решения и даже выполнять творческие задачи. Вместе с тем, широкое внедрение ИИ несет в себе не только огромные возможности, но и новые вызовы, особенно в области безопасности и уголовного права. С развитием и усложнением технологий ИИ возрастает и потенциальный риск их использования в преступных целях. Современные киберпреступники и злоумышленники находят все более изощренные способы применения искусственного интеллекта для реализации своих преступных замыслов. От создания фальшивых изображений и видео (deepfake) до автоматизированных кибератак, мошенничества и манипуляции общественным мнением – ИИ становится мощным инструментом, который может использоваться не только во благо, но и во вред обществу.

Тематика использования ИИ в качестве орудия преступления становится особенно актуальной в условиях стремительного цифрового преобразования мира и все большей зависимости от информационных технологий. Киберугрозы, связанные с ИИ, приобретают новые формы и масштабы, что вызывает серьезные опасения у специалистов по безопасности, правоохранительных органов и законодателей. Понимание природы этих угроз, изучение реальных случаев преступного применения ИИ, а также разработка эффективных мер противодействия – важные задачи современного общества.

Искусственный интеллект (ИИ) – это область компьютерных наук, связанная с созданием систем и программ, способных выполнять задачи, требующие человеческого интеллекта. К таким задачам относятся распознавание речи, обработка естественного языка, принятие решений, обучение и адаптация, распознавание образов, планирование и решение проблем.

Существует множество определений ИИ, отражающих различные подходы к пониманию и реализации искусственного интеллекта. Одним из классических

является определение, данное Джоном Маккарти – одним из основателей этой области, - который описывал ИИ как «науку и инженерию создания интеллектуальных машин, особенно интеллектуальных компьютерных программ». Это определение подчеркивает как научный, так и инженерный аспекты ИИ. В зависимости от уровня развития и функциональности искусственный интеллект можно классифицировать на несколько типов:

- узкий (или слабый) ИИ – системы, разработанные для выполнения конкретных задач. Например, голосовые помощники, системы распознавания лиц, рекомендательные алгоритмы. Они эффективны в строго определенных областях, но не обладают общей способностью к мышлению и обучению вне заданной сферы.
- общий (или сильный) ИИ – гипотетический тип ИИ, который мог бы выполнять любые интеллектуальные задачи, доступные человеку, включая способность к осмыслению, самообучению и творчеству. На сегодняшний день такой уровень ИИ остается предметом теоретических исследований и футуристических прогнозов.
- суперинтеллект – это концепция ИИ, превосходящего человеческий интеллект во всех сферах. Суперинтеллект пока что – объект спекуляций и обсуждений этических и философских вопросов.

История искусственного интеллекта начинается в середине XX века с появления первых программ и алгоритмов, имитирующих интеллектуальные функции. В 1956 году на конференции в Дартмутском колледже впервые был официально введен термин «искусственный интеллект», положивший начало целому научному направлению. Первые успехи в области ИИ связаны с разработкой логических и символических систем, способных решать ограниченные задачи. Однако уже к 1970-м годам стало ясно, что символический ИИ не способен эффективно работать с неопределенностью и сложностью реального мира. С 1980-х годов начинается эра методов машинного обучения, основанных на статистических моделях и больших объемах данных. В 2010-х благодаря развитию вычислительных мощностей и накоплению огромных данных получил развитие глубокий машинный интеллект – глубокие нейронные сети, которые сегодня лежат в основе многих современных приложений ИИ.

Современный искусственный интеллект включает широкий спектр технологий и методов:

-машинное обучение (ML) – алгоритмы, которые обучаются на данных, выявляя закономерности и принимая решения без явного программирования каждого шага. Среди них популярны методы классификации, регрессии, кластеризации.

- глубокое обучение (Deep Learning) – подвид машинного обучения, основанный на многоуровневых нейронных сетях. Позволяет решать сложные задачи, такие как распознавание речи, изображений и обработка естественного языка.

- обработка естественного языка (NLP) – технологии, обеспечивающие взаимодействие человека и компьютера с помощью текста и речи, включая перевод, анализ тональности, генерацию текста.

- компьютерное зрение – системы, способные воспринимать и интерпретировать визуальную информацию, используемую в распознавании лиц, автономных транспортных средствах и медицинской диагностике.

Помимо деления на узкий и общий ИИ, искусственный интеллект классифицируется по функциональным возможностям и уровню автономии:

- Реактивные машины (Reactive Machines) – самые простые ИИ-системы, которые не имеют памяти и не могут использовать предыдущий опыт для принятия решений. Они реагируют исключительно на текущие входные данные. Пример – шахматная программа IBM Deep Blue, которая анализировала позиции на доске без учета истории ходов.

- ограниченная память (Limited Memory) – такие системы способны учитывать опыт, полученный за определенный период времени, чтобы улучшить текущие действия. Большинство современных ИИ, включая системы автономного вождения и распознавания речи, относятся к этой категории.

- теория разума (Theory of Mind) – это гипотетический уровень ИИ, который подразумевает понимание эмоций, намерений и мыслей других агентов – будь то люди или машины. Такой ИИ сможет взаимодействовать более естественно и эффективно, учитывая психологические и социальные аспекты.

- самосознание (Self-aware AI) – самый высокий и пока что недостижимый уровень, когда машина обладает собственным сознанием и самосознанием. Теоретически такие системы смогут анализировать свои состояния и корректировать поведение на основе этого анализа.

ИИ-системы демонстрируют впечатляющие способности, но имеют и свои ограничения, которые важно учитывать:

-автоматизация рутинных и повторяющихся задач, повышая эффективность и снижая издержки.

-обработка больших объемов данных и выявление скрытых закономерностей, недоступных человеку.

-повышение точности диагностики в медицине, прогнозирования и управления процессами.

- создание новых форм коммуникации и персонализации сервисов.

-зависимость от качества и объема обучающих данных – ошибки или предвзятость данных могут привести к неверным решениям.

-отсутствие истинного понимания и контекста – ИИ оперирует шаблонами, а не смыслом.

-риск неправильного применения или злоупотребления, особенно в сферах с высокой степенью ответственности.

-этические и социальные дилеммы, связанные с приватностью, автономией и воздействием на рынок труда.

Угрозы и вызовы, связанные с использованием ИИ.

Развитие искусственного интеллекта открывает не только новые возможности, но и значительные риски, связанные с его потенциальным использованием в преступных целях. ИИ становится мощным инструментом в руках злоумышленников, способным автоматизировать и совершенствовать методы преступной деятельности, а также создавать качественно новые виды угроз. Ключевые угрозы связаны с тем, что ИИ способен:

- обрабатывать и анализировать огромные объемы информации с высокой скоростью, что позволяет осуществлять масштабные и точные атаки.

-генерировать реалистичный контент (тексты, изображения, аудио, видео), что усложняет обнаружение фальсификаций и манипуляций.

-автоматизировать процесс взлома, создавая адаптивные и самосовершенствующиеся методы атаки.

-использовать уязвимости в системах ИИ для обхода средств защиты и внедрения вредоносного кода.

Эти возможности приводят к возникновению новых форм киберпреступности, а также усложняют традиционные преступные схемы, расширяя их масштаб и эффективность.

Использование искусственного интеллекта в криминальной деятельности можно условно разделить на несколько ключевых направлений:

Киберпреступления: взломы компьютерных систем, кража данных, проведение распределённых атак отказа в обслуживании (DDoS), фишинг и другие виды атак, в которых ИИ используется для автоматизации и повышения эффективности. Например, ИИ может подобрать пароли быстрее или создавать более убедительные фишинговые письма.

Мошенничество и социальная инженерия: использование ИИ для создания поддельных голосовых сообщений (в том числе deepfake-аудио), автоматического генератора фальшивых текстов и переписок, что позволяет вводить жертву в заблуждение и получать доступ к конфиденциальной информации или финансам.

Манипуляция информацией: создание и распространение фальшивых новостей, изображений и видео, влияющих на общественное мнение, политические процессы или экономику. Технологии deepfake позволяют практически неотличимо подделывать видеоконтент.

Автоматизация преступных операций: использование ИИ для управления ботнетами, координации незаконных действий и скрытого мониторинга жертв.

Криминальное использование робототехники и автономных систем: применение автономных дронов и роботов в преступных целях, например, для контрабанды или проведения атак. Использование искусственного интеллекта в преступных целях обладает рядом специфических особенностей, которые отличают такие преступления от традиционных форм нарушения закона. Понимание этих особенностей необходимо для эффективного противодействия и разработки адекватных мер безопасности.

Автоматизация и масштабируемость. Одним из ключевых преимуществ ИИ является возможность автоматизировать сложные и трудоемкие процессы, что в криминальном контексте позволяет масштабировать атаки и значительно увеличивать их эффективность. Например, использование машинного обучения для генерации фишинговых сообщений позволяет рассылать миллионы персонализированных писем, существенно повышая шансы обмана.

Адаптивность и самообучение. Современные ИИ-системы могут самостоятельно анализировать результаты своих действий и корректировать поведение в реальном времени. В контексте преступлений это означает, что атаки могут становиться более изощренными и менее предсказуемыми, адаптируясь к изменениям систем защиты и поведению жертв.

Высокий уровень маскировки и сокрытия следов. ИИ способен создавать высококачественные фальсификации – аудио, видео и текст, которые трудно отличить от оригинала. Это затрудняет идентификацию злоумышленников и проведение расследований, поскольку доказательства могут быть искусственно созданы и подложны манипуляциям.

Сложность правового регулирования и определения ответственности. Использование ИИ в преступных схемах поднимает сложные вопросы юридической ответственности. В частности, затрудняется определение субъекта преступления, особенно если ИИ действует автономно или создаётся третьими лицами. Это требует адаптации законодательной базы и развития международного сотрудничества.

Низкая стоимость входа и доступность технологий. Ранее сложные и дорогие технологии ИИ становятся всё более доступными благодаря развитию облачных сервисов, открытым библиотекам и платформам. Это приводит к тому,

что злоумышленники с минимальными ресурсами могут использовать продвинутые ИИ-инструменты для реализации преступных целей.

Международный и трансграничный характер преступлений. Киберпреступления с использованием ИИ часто не ограничиваются одной юрисдикцией. Это создаёт сложности для правоохранительных органов, которые должны координировать действия с международными партнёрами для расследования и пресечения подобных преступлений.

ИИ всё чаще используется злоумышленниками для усовершенствования кибератак. Он помогает автоматизировать взломы, генерировать вредоносный код, обходить системы защиты и анализировать данные жертв. Ниже представлены яркие примеры.

Пример 1. Взлом с использованием ИИ-поддерживаемых фишинговых писем. Ранее фишинг основывался на шаблонных сообщениях, легко распознаваемых как мошеннические. Современные языковые модели, такие как GPT, позволяют создавать грамматически правильные, персонализированные письма, которые трудно отличить от настоящих. В одном из зафиксированных инцидентов, ИИ был использован для генерации фишинговых e-mail от имени генерального директора компании. Письмо было персонализировано под получателя, включало реальные детали проектов и достигло высокой степени доверия. Потери компании составили более 200 000 долларов.

Пример 2: атаки на корпоративные системы с помощью ИИ-пентестеров. Существуют инструменты, основанные на ИИ, которые действуют как «автоматизированные пентестеры» - они ищут уязвимости в корпоративных сетях, адаптируясь к системе защиты. Такие технологии используются как в легальных целях (тестирование безопасности), так и преступниками. В одном случае ИИ нашёл нестандартную уязвимость в старом API корпоративного банка, и использовался для кражи конфиденциальных данных.

Пример 3: Deepfake-голос, имитирующий звонок от руководителя. В 2020 году в Великобритании был зафиксирован случай, когда финансового директора заставили перевести 240 000 евро, думая, что он разговаривает с генеральным директором головной компании. На самом деле голос был сгенерирован с помощью ИИ и звучал настолько правдоподобно, что вызвал полное доверие у жертвы. ИИ позволяет манипулировать доверием и восприятием людей на принципиально новом уровне. Технологии синтеза речи, генерации текста и анализа социальных сетей позволяют создавать реалистичные образы и истории.

Пример 4: ИИ, анализирующий соцсети для персонализации атак. Мошенники применяют ИИ для сбора открытых данных о людях – привычках, интересах, деловых связях. Затем генерируют «нативные» сообщения,

основанные на интересах жертвы, чтобы ввести в заблуждение (например, от имени коллеги, ссылающегося на общий проект или личное увлечение).

Искусственный интеллект открывает перед человечеством огромные возможности, но одновременно создает новые угрозы и вызовы. Использование ИИ в преступных целях становится все более изощренным и масштабным, требуя от общества и государственных институтов эффективного и своевременного реагирования. Только комплексный подход, объединяющий технические, правовые и этические меры, позволит минимизировать риски и сохранить технологии ИИ в рамках служения на благо.

Список использованной литературы

1. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. Классический учебник по ИИ, охватывающий как основы, так и современные достижения.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. Основополагающий труд по глубокому обучению, одной из ключевых технологий ИИ.
3. Brundage, M., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Доклад, посвященный потенциальным злоупотреблениям ИИ и способам борьбы с ними.
4. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. Книга о проблемах безопасности данных и приватности, актуальных в эпоху ИИ.
5. Taddeo, M., & Floridi, L. (2018). How AI Can Be a Force for Good. Science, 361 (6404), 751-752. Статья, рассматривающая этические аспекты использования ИИ.