Список использованных источников

1. Что представляет собой искусственный интеллект? [Электронный ресурс]. — Режим доступа https://www.sap.com/ — Дата доступа: 09.11.2023.

2. Machine Learning [Электронный ресурс]. — Режим доступа: https://bigdataschool.ru/wiki/machine-learning/ — Дата доступа: 09.11.2023.

УДК 004.896

А.В. Ивановский, К.Н. Слободчиков,
Академия управления при Президенте Республики Беларусь
Минск, Беларусь

КРИМИНОЛОГИЧЕСКИЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

***Аннотация**. Искусственный интеллект стал неотъемлемой частью нашей жизни, однако его использование в преступных целях вызывает серьезную озабоченность. Важно разрабатывать стратегии защиты от подобного рода преступности и предотвращать злоупотребление ИИ для незаконных целей.*

A.V. Ivanovsky, K.N. Slobodchikov
The Academy of Management under the President of the Republic of Belarus
Minsk, Belarus

CRIMINOLOGICAL DIRECTIONS OF ARTIFICIAL INTELLIGENCE USE

***Abstract.** Artificial intelligence has become an integral part of our lives, however, its use for criminal purposes raises serious concerns. It is important to develop strategies to protect against such criminal activities and to prevent the abuse of AI for illegal purposes.*

В настоящее время искусственный интеллект (ИИ) вышел за пределы научных исследований. Он интегрировался в экономику, технологические отрасли промышленности, сферу услуг [1].

Согласно экспертным оценкам, в течение ближайших 15 лет потенциальную опасность будут представлять три группы угроз применения ИИ в преступных целях, которые условно обозначены как самые опасные, средней опасности и наименее опасные.

Ранжирование осуществлялось на основании следующих критериев: причиняемый вред, возможность получения преступной прибыли или выгоды, насколько легко может быть совершено преступление и насколько трудно будет его предотвратить.

К числу «самых опасных» были отнесены дипфейки и роботизированные устройства с использованием инструментов ИИ. Хотя само слово «дипфейк» звучит менее тревожно, чем, скажем, «робот-убийца», эта технология на данный момент самая реальная криминальная киберугроза в силу того, что она более доступна, способна очень легко причинить большой вред, ее также трудно обнаружить и остановить [2].

Дипфейк – технология обработки контента, которая подменяет лицо и голос человека с помощью инструментов ИИ. Обычно называемые формой «синтетических медиа», дипфейки имитируют лица, движения и голоса людей с такой точностью, что их часто невозможно отличить от оригинала в реальной жизни без специальных инструментов.

Благодаря высокоразвитым алгоритмам машинного обучения можно манипулировать такими биометрическими параметрами, как выражение лица и тон человеческого голоса, чтобы создавать реалистичное изображение событий, которые никогда не происходили.

Используя поддельные аудио и видео с целью выдать себя за другого человека, можно причинить различные виды вреда: от дискредитации до вымогательства финансовых средств.

Криминальная ситуация осложняется тем, что уже есть ресурсы, где можно создать дипфейки онлайн без специальных знаний.

Дипфейки представляют собой растущую криминальную угрозу, а дипфейк-преступления постепенно становятся «общим достоянием» [3]. По мере того, как эти технологии делаются более доступными и качественными, им труднее противодействовать. Хотя некоторые алгоритмы успешно идентифицируют дипфейки в Интернете, существует множество неконтролируемых путей распространения модифицированных материалов. Это может привести к повсеместной дискредитации аудио-и визуального контента.

К первой группе криминальных угроз также относятся приложения ИИ, связанные с робототехникой.

В преступных целях стали применяться беспилотные летательные аппараты, автоматизированные транспортные средства, управляемые с помощью инструментов ИИ [4].

Преступники используют их, например, для контрабанды наркотиков, оружия и контрафактной продукции. В некоторых случаях

дроны применяют для разведки, например, при подготовке кражи или разбойного нападения, поскольку с их помощью можно установить график пребывания хозяев или охраны на объекте, привычки владельцев, расположение камер, количество людей и т.д.

Дроны признаны также действенным механизмом доставки взрывчатых веществ или даже самостоятельным оружием террора. Сюда также относятся уже разработанные снайперские винтовки дальнего действия с джойстиками для управления, которые заметно снижают требования к профессиональной подготовке киллеров и боевиков.

Кроме того, происходит увеличение количества систем ИИ третьей волны, используемых для ключевых приложений обеспечения общественной безопасности, а также на многочисленные возможности для атак, которые они представляют.

Нарушение работы таких систем, контролируемых ИИ, по преступным мотивам может привести к массовым отключениям электроэнергии, нарушению логистики продовольствия и общему хаосу.

Ко второй группе относятся так называемые многокомпонентные киберугрозы криминального характера с использованием ИИ. Одна из таких угроз – фейковые платежные системы, способные совершать автоматизированные мошеннические транзакции посредством алгоритмов машинного обучения и анализа больших данных.

Ключевой драйвер роста – это партнерские программы. Их используют продавцы доступов в скомпрометированные сети и интернет-мошенники.

Распространение получили ориентированные на страны СНГ фишинговые и мошеннические программы, программы-вымогатели.

В связи с этим велика вероятность роста утечек биометрических данных из государственных структур, происходящих в результате действий внутренних нарушителей. Биометрические способы идентификации и аутентификации применяются все шире, в том числе для получения доступа к финансовым сервисам.

Можно отметить, что вредоносное программное обеспечение усложняется, становится более «интеллектуальным», моделирующим поведенческие факторы онлайн-пользователей и использующим психологические методы социальной инженерии.

По механизмам и способам преступные деяния, совершаемые с использованием таких технологий, вариативны, имеют высокий уровень латентности и трансграничный характер. Кроме того, вредоносные программы содействуют сращиванию преступных групп

и сообществ, организованные транснациональные альянсы которых приводят к эскалации криминальных киберугроз. В них задействовано большое количество участников, есть строгая иерархия и сложная техническая инфраструктура.

Подобные системы используются, в том числе, для прикладных задач хакеров, меняя в ходе функционирования свою направленность, – не привлекающий сегодня внимание пользователя майнер может завтра превратиться в банковский вирус.

Крупные хакерские группировки совершают целенаправленные масштабные атаки на банки, государственные и бизнес-структуры, пытаются выходить на новые рынки. Интерес киберпреступников стали привлекать крупные криптоплощадки. Злоумышленники все больше внимания обращают на пользователей мобильных телефонов и смартфонов.

Наконец, к последней группе криминальных угроз с использованием ИИ относятся «наименее опасные».

Среди них – создание и распространение вредоносных программ и технологий, направленных как на нарушение правил этического кодекса интернет-взаимодействия, так и на противоправные деяния.

Создание сайтов с негативными публикациями и фальшивыми отзывами – это всего лишь один из примеров того, что может делать самообучающийся ИИ.

Таким образом, так называемые «грязные» цифровые технологии, по нашему мнению, эволюционируют от мелкого психологического насилия в социальных сетях до одного из самых эффективных виртуальных инструментов PR-технологий и пропаганды, который применяется, в частности, в недобросовестной борьбе с конкурентами, при создании и регулировании искусственного спроса на определенные товары и услуги.

Ожидается, что до 2025 года будет наблюдаться устойчивое развитие рынка технологий ИИ.

На основании изложенного, в качестве приоритетных направлений можно определить: – создание инструментов гибкого этического и правового регулирования процессов развития и функционирования ИИ на международном уровне; – обеспечение комплексной и эффективной защиты прав интеллектуальной собственности от несанкционированного использования третьими сторонами ИИ, а также патентование результатов научной деятельности в этой сфере;

– разработку и реализацию новых решений, конкретных мер, направленных на предупреждение и пресечение криминальных угроз с

использованием ИИ; – развитие и совершенствование системы международного обмена информацией об угрозах и способах совершения преступлений с использованием технологий ИИ; – подготовку профессиональных кадров, формирование компетенций, которые позволят повысить эффективность противодействия применению ИИ в преступных целях; – проведение мониторинга, совместных научных исследований в области борьбы с существующими, а также новыми и зарождающимися криминальными угрозами с использованием технологий ИИ.

Список использованных источников

1. https://issek.hse.ru/news/830132491.html.
2. https://mediabrest.by/news/tehnologii/novaya-ugroza-ot-tehnologiy-kriminalnaya-zhizn-dipfeykov.
3. https://forklog.com/news/ai/sotrudnik-microsoft-dipfejki-predstavlyayut-soboj-rastushhuyu-ugrozu.
4. https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-prestupnyh-tselyah-metody-protivodeystviya-i-borby.

УДК 004.021

В.В. Смелова, Д.В. Шиман
Белорусский государственный технологический университет
Минск, Беларусь

МЕТОД ПОСТРОЕНИЯ КОНСОЛИДИРОВАННОГО ПЛАНА ВАЛОВОГО ОБЪЕМА ПРОДУКЦИИ ПРОМЫШЛЕННОГО КЛАСТЕРА

Аннотация. *Статья посвящена методу планирования совместной деятельности участников промышленного кластера на основе балансовой модели В.В. Леонтьева. При пошаговом построении плана участники кластера вносят изменения в свои локальные планы и согласуют параметры планов с другими участниками. Результатом является согласованный всеми участниками план валового объема продукции кластера.*

V.V. Smelova, D.V. Shiman
Belarusian State Technological University,
Minsk, Belarus