Волков Геннадий Юрьевич
канд. экон. наук, доцент
ФГКОУ ВО «Ростовский юридический институт МВД России»
г. Ростов-на-Дону, Ростовская область

САМОРАЗВИТИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА КАК ОСНОВНАЯ УГРОЗА ДЕСТАБИЛИЗАЦИИ НАЦИОНАЛЬНОГО СОЦИУМА В УСЛОВИЯХ ПРОКСИ-ВОЙНЫ С ГЛОБАЛЬНЫМ ЗАПАДОМ

Аннотация: *в статье предпринята попытка анализа основных проблем, связанных с неконтролируемой возможностью самосовершенствования искусственного интеллекта и тенденциями его использования в оказании деструктивного воздействия на потенциального конкурента в условиях ускоренной цифровизации.*

Ключевые слова*: виртуальное пространство, искусственный интеллект, цифровизация, национальное государство, социальная инженерия, CMS, NLB, UHG.*

С самого начала XX века важнейшими катализаторами развития мирового производственного комплекса окончательно становится НТР и НТП, определившие в качестве важнейшего фактора сохранения конкурентоспособности возможность перманентной модернизации реального сектора. Развитие индустриального способа производства, основанного на определяющей роли технологической составляющей, позволяло постоянно расширять номенклатуру товаров с высокой долей добавленной стоимости, что и определяло место национального государства в системе мирохозяйственных связей. Качественные последствия трансформации производственной сферы в конечном итоге привели к запуску механизма глобализации мировой экономики.

В итоге появилась реальная возможность структурировать внешнеторговую политику и внешнеэкономическую деятельность с максимальным учетом субъ-

ективных целей. Негласный союз крупнейших ТНК с национальными административными структурами позволил осуществлять финансово-экономическую экспансию, на территорию национального государства для установления необходимого контроля над конкурентами. Развитие процессов глобализации в числе прочих трансформационных изменений позволило подготовить предпосылки для перехода ряда стран на постиндустриальный уровень, на котором определяющую роль начинает играть информационно-технологический фактор [1].

По мере углубления трансформационных изменений, большинство из которых имеют необратимый характер, процесс конкуренции начинает приобретать все более жесткие и неординарные формы нейтрализации конкурента. Одной из форм воздействия на потенциального потребителя стало появление социальной инженерии, задачей которой стало форматирование общественного сознания и поведенческой модели индивида в заданном направлении. От того, насколько национальный социум способен воспринимать, анализировать и использовать полученную информацию, зависит в конечном итоге не только сохраняемых позиций в мировой архитектуре, но сохранение должного уровня социальной стабильности, контроль над которой начинает осуществлять внешний фактор [2].

Одним из направлений постиндустриальной науки стали разработки в сфере использования ИИ (искусственного интеллекта) для облегчения обработки растущих потоков информации, создания вариативных управленческих стратегий, координации производственных процессов и т. д. Однако проблематика использования ИИ сразу заинтересовала не только представителей крупного бизнеса, но и социальных инженеров и военных. Фактически речь идет о дополнительном эффективном факторе ведения прокси-войны с потенциальным противником, что и было доказано после начала СВО.

Западные кураторы украинского режима практически не скрывают своей главной задачи – нанести максимально возможный урон информационным структурам российского государства, и по возможности вывести из строя структуру управления

В противостояний с РФ, коллективный Запад возлагает на систему ИИ большие надежды, поскольку даже самые элементарные генераторы контента, такие как *ChatGPT* – прототип чат-бота с искусственным интеллектом или мультимодальная модель ИИ *Gemini,* которая способна анализировать, обрабатывать и комбинировать различные типы аудио и видео информации, позволяют активно воздействовать на индивидуальное сознание. Украинские оператор-хакеры под руководством зарубежных кураторов активно используют предоставленные возможности для генерирования и распространения дезинформации и фейковых новостей и мошеннических телефонных атак. Целью последних является получение персональных данных, конфиденциальной и секретной информации и т. п.

Согласно представленным данным Роскомнадзора, около 90% утечек непосредственно связаны с действиями украинских хакеров, которые используют уязвимости в CMS, не обновляемых вовремя системными администраторами. В числе наиболее активных украинских хакерских групп необходимо выделить NLB, UHG и IT Army of Ukraine. Оосбую тревогу вызывает постоянный рост деструктивной активности белорусской хакерской группы «Киберпартизаны».

Совершенствуя ранее сгенерированные программы, ИИ самостоятельно начинает создавать фейковые контенты в поисковых системах Сети, что значительно усложняет определение степени достоверности информации. Согласно отчетам аналитиков, в Сети уже существует 725 веб-сайтов, степень надежности которых характеризуется как минимальная. Особенностью данных сайтов является то обстоятельство, что они полностью сгенерированы ИИ, без какого-либо участия, а, главное контроля со стороны человека.

Аналитики особо обращают внимание на то обстоятельство, что такая распространенная система как GOOGLE активно экспериментирует с инструментами ИИ для предоставления издателям возможности обобщения информации из внешних источников. Однако обратной стороной этого процесса является резкое снижение степени достоверности и надежности онлайн-контента. О скорости саморазвития ИИ можно судить по тому факту, что генеративный ИИ начинает со-

здавать мультимедийный контент, что значительно повышает степень «достоверности» сгенерированной подделки. Это уже начинает вызывать серьезные опасения у администраторов большинства платформ, особенно социальных сетей. В качестве защитных мер используется вариант отфильтровывания квазиконтентов с возможностью последующей блокировки. В этой связи одной из важнейших рекомендаций становится постоянное повышение медиа-грамотности населения с формированием аналитических способностей, позволяющих исключать возможность доверия сомнительной информации. В числе самых простых решений предлагается проверять полученную информацию с использованием альтернативных информационно-справочных источников [3].

Большую тревогу вызывает отказ от любых контактов с российским сегментом со стороны западных коллег в сфере международной информационной безопасности для предотвращения киберпреступлений в виртуальном пространстве. Фактически противостояние в сегменте кибербезопасности после начала СВО достигло своего апогея. Вместо конструктивных мер по предотвращению негативных составляющих, коллективный Запада фактически начал активное использование ИИ для достижения задач социальной инженерии по дестабилизации российского социума. И первым этапом этой борьбы стало открытое противостояние в виртуальном пространстве.

Несмотря на опасения ученых, начинается активная интеграция ИИ практически во все сегменты функционирования современных мирохозяйственных связей. Используемые инструменты генеративного ИИ постоянно совершенствуются, что начинает вызывать все больше опасений, поскольку скорость самосовершенствования и снижение, вплоть до блокировки, сторонних контрольных функций начинают проявляться все чаще.

Список литературы

1. Альпидовская М.Л. Искушение «большой цифрой»: «инклюзивный капитализм», или общество постмодерна / М.Л. Альпидовская, А.М. Корнилов. – М.: ИНФРА-М, 2024. – 184 с. – ISBN 978-5-16-018470-8. – DOI 10.12737/2009647. – EDN SJBHXS.

2. Бахтин М.В. Искусственный интеллект и новый технологический уклад / М.В. Бахтин // Человек в современном мире: искусственный и естественный интеллект: соперничество или соработничество?: сборник научных трудов. – Рагуза: Энциклопедист-Максимум, 2024. – С. 13–26. – EDN XGISOH.

3. Пылов П. А. Изучение искусственного интеллекта на основе принципа интенсификации обучения / П.А. Пылов, Р.В. Майтак, А.В. Дягилева. – Вологда: Инфра-Инженерия, 2024. – 172 с. – ISBN 978-5-9729-1594-1. – EDN YFPIKU.