Нидентaль Андрей Евгеньевич
студент
Поволжский институт управления имени П.А. Столыпина –
филиал ФГБОУ ВО «Российская академия
народного хозяйства и государственной службы
при Президенте Российской Федерации»
г. Саратов, Саратовская область

ПРОБЛЕМЫ ОТСУТСТВИЯ ДЕТАЛЬНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

Аннотация*: статья посвящена проблеме использования киберпреступниками технологий искусственного интеллекта. В статье рассматривается роль использования различных разновидностей нейросетей. Также акцентируется внимание на том, что на сегодняшний день в законодательстве РФ отсутствует должный объём информации, что касается использования технологий искусственного интеллекта. Также в статье рассматривается примеры зарубежного опыта ЕС, США, КНР в этой сфере. Также в статье приводится предложение для изменений и нововведений в законодательство РФ по устранению правовых проблем ИИ.*

Ключевые слова*: искусственный интеллект, нейросеть, дипфейк, генерация текста, цифровизация, спам, киберпреступность, кибермошенничество, реформирование законодательства.*

Уже давно в мире в целом, так и в России в частности идёт широко распространяющиеся цифровизация. Она охватывает все стороны человеческого общества. Начавшись как экспериментальный военный проект интернет стал общедоступным и обязательным инструментом повседневной жизни современного человека [1].

Цифровизация ускорила процесс передачи информации между людьми. Для простоты такую информацию можно разделить на политическую, экономическую, научную и социокультурную [2]. Изначально цифровизация шла с ходом появления

и распространения компьютерных технологий и аппаратуры. А с недавнего времени к такому технологическому прогрессу прибавилось появление и стремительное развитие искусственного интеллекта (ИИ), в частности нейросетей [3].

Такие процессы повлекли резкий скачок создания различного контента в социальных сетях. Простота и масштабность процесса изготовления нейросетевого контента стала иметь как положительные, так и отрицательные последствия для общества [4]. Интерес настоящей статьи прикован именно на негативные последствия. На данный момент негативные последствия характеризуются фактом распространением в массовом характере мошеннического и вульгарного контента, как правило нацеленного на пожилых и несовершеннолетних пользователей, плохо знакомых правилами нахождения в интернете.

Это делает тему вопроса борьбы с нейросетевым видом киберпреступности крайне актуальной. Под нейросетевым видом киберпреступности подразумевается использование различных нейросетей в преступных целях в сетевом пространстве интернета. Но стоит дать определению тому, что мы называем нейросетью. Толковый словарь Ожегова говорит о том, что нейросеть – это: «Математический алгоритм, созданный и работающий по принципу нейронных сетей живых организмов, их нервных клеток. А также реализация данной модели в программе». Однако у понятия нейросети существует огромное количество вариаций. Различаются они по многим вопросам. Эти вопросы как правило заключаются в области применений той или иной нейросети [5].

Резкое появления и развитие нейросетей стало очень удобным полем для незаконной деятельности. Связанно это с тем, что государство не успевает реагировать посредством законотворчества на такую проблему, как нейросетевая киберспеструпность. А само общество как правило не имеет культуры взаимодействия с таким новым явлением. Все эти факторы способствуют неконтролируемому ущербу различным общественным институтам со стороны киберпреступников.

Именно кибермошенничество заняло большое место в проценте преступлений нейросетями. Нейросети помогают злоумышленниками крайне быстро эмулировать различные человеческие навыки и действия в области организации преступной

деятельности. Они могут успешно создавать варианты путей для злоумышленников в их противоправном деле. Нейросети способны к обучению. Причем это обучении как правило начинает проходить самостоятельно с определённого момента, когда база данных нейросети становится достаточной для этого [6].

Нейросети могут действовать во вред обществу. И их действия в основном проявляются в генерация Аудиовизуального контента. Это, пожалуй, самое главное из разновидностей действий нейросетей. В преступном направлении они способны генерировать текст, который вводит пользователя в заблуждение. В этом они крайне хорошо способны копировать манеру написании текста тех или иных людей, выдавая себя за них. Также эта способность хорошо ложится на умение генерации паролей для различных сервисов. Они способны генерировать купоны, дающие право на получении скидки на товары. Способны генерировать ключи, для бесплатного получения товаров.

Помимо простого создания текста, нейросети могут создавать изображения и видео [7]. Именно изображения как правило становятся характерным почерком массового спама в социальных сетях. Нейросети как правило создают их исходя из уже полученного собственного опыта. То есть, они анализируют то, какие посты в тех или иных социальных сетях набирали больше просмотров и реакций, и используют те вводные слова для генерации, которые были использованы на тех постах. Как правило к этому они создают различные дополнения в целях усиления эффекта от постов. Из-за таких дополнений изображения генерируются нейросетями принимают крайне сюрреалистически внешний вид. В этих изображениях часто фигурируют такие сюжеты как: бедные африканские дети, собирающие из мусора различные скульптуры, американские ветераны-инвалиды, просящие милостыню у прохожих, различные изображения Иисуса Христа, а также других религиозных персонажей и символики. Все они рассчитаны на получения различных реакций. Эти изображения могут распространяются в виде постов с ссылками, ведущими на мошеннические и вредоносные сайты. А также эти изображения используются для привлечения трафика на аккаунты, распространяющие эти изображения. После чего данные аккаунты могут быть подвергнуты продаже.

Также такие изображение могут иметь эротический и порнографический характер, что, как пример, противоречит законодательству РФ [8].

Такая проблема массово распространяется в виде спама по зарубежным социальным сетям, некоторые из которых в свою очередь были признаны экстремистскими и террористическими на территории РФ.

Подобный спам как правило рассчитан на людей плохо знакомых с культурой поведения в интернете. Такими людьми являются как правило пожилые и несовершеннолетние, которые как правило происходят из стран Запада. Именно они являются целевыми жертвами киберпреступников из-за того, что имеют как правило более финансово обеспечены.

Также стоит отметить, что управление такими аккаунтами, распространяющими нейросетевой спам, также осуществляется нейросетями. Такие аккаунты можно отнести к вредоносным ботам, что проводят социоинженерные атаки на пользователей. Эти аккаунты как правило являются специально созданными для такой деятельности. Они могут иметь при себе изображения настоящих людей, и даже выдавать себя за них, используя также и их имена. Такие аккаунты как правило крайне активные в плане создания постов. И часто они стремятся установить контакт с аккаунтами настоящих людей [9].

Наряду со спамом изображений существует проблема дипфейка. Это технология, позволяющая в режиме настоящего времени менять лицо человека на любое другое. Данная тактика преступлений позволяет злоумышленникам более успешно вводить своих потенциальных жертв в заблуждение. А также через экран смартфона не всегда получается успешно определить наличие дипфейка [10]. Эта проблема усиливается тем, что замена своего лица на чужое на данный момент никак не контролируется законодательством. В законодательстве до сих пор отсутствует понятие дипфейка [11].

С этой технологией идёт и изменение голоса через нейросеть. Нейросети с недавнего времени способны менять голос человека под любой другой, если у него имеется данный для имитации того или иному конкретного голоса. Как и в

случае внешности человека. В законодательстве нет регуляции права на человеческий голос. Это позволят злоумышленникам свободно использовать изменение речи через нейросеть [12].

Все эти и тому подобные действия киберпреступников не могут оставаться без ответа со стороны государства. В законодательстве РФ существует определение искусственного интеллекта. Оно приводится в Федеральном Законе от 24 апреля 2020 года №123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Данное определение заключается в том, что ИИ – это комплекс технологических решений, способных имитировать когнитивные функции человека, в частности самообучение и генерацию результата, сопоставимого с результатом интеллектуальных усилий человека [13].

Также подобное отношение к ИИ со стороны нашего государства было выражено годом ранее в Указе Президента РФ от 10 октября 2019 г. №490 «О развитии искусственного интеллекта в Российской Федерации» [14].

Помимо данных НПА в РФ существуют ГОСТы по ИИ [15]. Также в РФ существует Кодекс этики в сфере искусственного интеллекта. Однако он скорее направлен на гипотетическое будущее и имеет весьма теоретический общий характер, что не подходит для какого-либо прикладного применения.

Проблема заключается в том, что наше государство пытается охватить законодательным путём всё, что в общественном сознании относят к ИИ. И это касается и нейросетей. Попросту говоря конкретное определения нейросетей и других их частных проявлений отсутствует в законодательстве РФ.

Законодательство РФ просто не воспринимает вопрос ИИ детально. Слишком расплывчатое определение понятия ИИ в законодательстве может иметь положительные, так и отрицательные последствия для правового регулирования деятельности людей, при использовании нейросетей.

«Ряд исследователей обращает внимание на проблему отсутствия в российском законодательстве юридических терминов «дипфейк», «нейросеть» и необходимость установления четких правил их использования путем принятия отдельного федерального закона», – отмечает Николай Титов, адвокат, соучредитель юридической компании a.t.Legal.

На этом следует обратить взгляд за рубеж с целью установления того, как иностранное законодательство в свою очередь реагирует и обуздывает проблемы, связанные с ИИ.

Первым примером можно выделить Европейский Союз. На его территории с весны 2024-го года действует Регламент об искусственном интеллекте (AI act). Данный регламент делит технологии на четыре категории исходя из того, какой риск представляет так или иная технология. В данном случае технологии – это то, что имется в основе работы ИИ. В четыре категории входит:

− недопустимый риск – запрещен социальный рейтинг и манипулятивный ИИ;

− высокий риск – системы, использующие ИИ в здравоохранении или при найме сотрудников, должны соответствовать строгим требованиям по качеству данных и управлению рисками;

− ограниченный риск – чат-боты и системы, генерирующие контент, должны информировать пользователей о взаимодействии с искусственным интеллектом;

− минимальный риск – системы вроде спам-фильтров и игровой ИИ не подпадают под строгие требования, для них действуют рекомендации.

Помимо категорий Регламент создаёт маркировку для объектов, что были созданы и ли подверглись обработке со стороны нейросетей.

Вторым примером с западного полушария стоит привести США. Там на национальном уровне ведётся регулирование вопросов, касающихся ИИ. Основной акцент ставится на обеспечение прозрачности при работе с ИИ, а также на безопасности при их эксплуатации. Октябрьским указом о безопасном, надежном и доверенном искусственном интеллекте Президент США установил те тре-

бования, которые раскрывают алгоритм, итоги тестирования и методы, что применяемы при создании технологий искусственного интеллекта. Данный указ также касается деятельности и провайдеров, что со своей стороны обязаны нести гарантии соблюдения прав человека, при ведении своей работы.

Упомянутый указ также, как и регламент ЕС подразумевает маркировку.

Третьим примером стоит взять опыт Китая. В КНР регулирование ИИ в основном акцентируется на поддержке политического единства страны и стабильности государства. В августе 2023-го вступили в силу «Временные правила оказания услуг с использованием ИИ». Основные требования, исходящие из данных правил, идут в сторону поставщиков услуг ИИ. В данных правилах сказано о безопасности, понятности соглашения, сохранении конфиденциальности, недопущения контента, противоречащего законодательству страны со своей стороны и стороны клиента

В частности, стоит отметить, что КНР в январе 2023-го года ввела положение касающегося ранее упомянутого дипфейка. Это связано с высокой популярности такой нейросетевой услуги в Китае. В положении приводится определение технологии, что стоит за функционированием дипфейка. Это определение гласит следующее: технология, использующая генеративные и/или синтетические алгоритмы, такие как глубокое обучение (deep learning) и виртуальная реальность, для создания текста, графики, аудио, видео или виртуальных сцен». Из этого можно сделать вывод о том, что определение является достаточно широким. Конечно, это можно считать негативной характеристикой. Однако, гипотетически такое широкое определение поможет в будущем быстрее и легче адаптировать законодательство, что увеличит скорость и качество реакции государства на появление и развитие технологий.

Также в этом положении стоит отметить то, что для поставщиков услуг дипфеков установлено требование мониторинга фейковых новостей, что создаются с использованием тех услуг дипфейка, что они поставляют.

Из китайского опыта можно сделать вывод, что установление более точных определений разновидностей преступной деятельности с помощью ИИ имеет место в практики иностранного законодательства [16].

Помимо иностранного опыта в судебной практике РФ также существует информация о том, как на данный момент в судебном производстве фигурируют проблемы, связанные с нейросетями. Как пример можно привести решение Новоильинского районного суда г. Новокузнецка по одному гражданскому делу декабря 2023-го года. В нём говорится, что злоумышленник воспользовался нейросетью изменяющею голос для того, чтобы ввести в заблуждение жертву, которая в свою очередь лишилась более трёх миллионов рублей в ходе совершения преступления.

Исходя из вышеизложенной ситуации следует со стороны государства прийти к тому, что создание отдельного Федерального закона, касающегося всех возможных вариаций существования и применений искусственного интеллекта должно быть реализовано. И его реализация желательно должна произойти в ближайшее время.

В таком гипотетическом НПА должны быть представлены как минимум все термины, которые используются на данный момент в обществе и в самом государстве. Помимо определения терминологии, следует установить точные меры взаимодействия государства с объектами, созданными нейросетями. Как пример можно использовать уже упомянутую маркировку. Также следует выявить государственное отношение к потенциальным будущем технология и свойствам по всем частностям сфер существования и применения искусственного интеллекта.

Помимо этого, стоит внести изменений, которые будут напрямую направлены на борьбу с незаконным применением технологии дипфейка. А именно внести такие изменение в части, касающейся защиты чести и достоинства, деловой репутации. В предложении таких мер можно отнести создание специальных общих ватермарок, что будут показывать наличие на том или ином изображении или видеофайле наличие использования дипфейка.

Нововедения и изменение должны также касаться и разработчиков ИИ. Примером могут служить опыт упомянутых в статье стран.

В заключении хочется сказать, что вопрос более детального регулирования действий киберпреступников при использовании ИИ является крайне важным и его важность усиливается с каждым днём. Так как процесс развития технологий и повсеместная цифровизация является всеобъемлющим фактором.

Список литературы

1. Авдыев Дж, Атаев М., Атаев С., Атадурдыева А. История возникновения интернета// Символ науки. 2023. №11–2-1.

2. Наталья Николаевна Плужникова, Светлана Викторовна Ковалева Цифровизация общества: техника, наука и нравственность // Векторы благополучия: экономика и социум. 2024. №4 (52).

3. Рупасов К. Р., Тесленко Е. А., Пионтковская С. А. Нейросеть CHATGPT: Революция в мире искусственного интеллекта // Вестник науки. 2024. №7 (76).

4. Алиев Тимур Фирудинович Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий // Юридические исследования. 2023. №10.

5. Ксенофонтов Вадим Валерьевич Нейронные сети // Проблемы науки. 2020. №11 (59).

6. Пикалов Павел Александрович, Бортников Сергей Петрович Кибермошенничество с использованием искусственного интеллекта // АВБсП. 2024. №2.

7. Голышева Е. Н., Медведев А. А., Масалитин Н. С., Ильинская Е. В. Основные подходы к генерации изображений с помощью нейронных сетей // Инновационная наука. 2023. №11–2. EDN WFMNUV

8. Литовченко Анна Игоревна Смоделированные изображения порнографического характера как предмет преступлений, связанных с обращением порнографии: компаративистское исследование // Вестник ЮУрГУ. Серия: Право. 2024. №2.

9. Коломеец М. В., Чечулин А. А. Метрики вредоносных социальных ботов // Труды учебных заведений связи. 2023. №1. DOI 10.31854/1813-324X-2023-9-1-94-104. EDN HEFHFR

10. Долгиева Мадина Муссаевна Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. 2024. №11 (168).

11. Бодров Николай Филиппович, Лебедева Антонина Константиновна Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. №11.

12. Белых Евгения Сергеевна, Грабчев Михаил Алексеевич К вопросу о введении уголовной ответственности за изготовление дипфейков в преступных целях// Право и управление. 2024. №5.

13. Федеральный закон "О проведении эксперимента по установлению специального регулиро-вания в целях создания необходимых условий для разработки и внедрения технологий ис-кусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных дан-ных" от 24.04.2020 N 123-ФЗ http://www.pravo.gov.ru

14. Указ Президента РФ от 10.10.2019 N 490 (ред. от 15.02.2024) "О развитии искусственного интеллекта в Российской Федерации" http://www.pravo.gov.ru

15. Гаврилова В. Д. Регламентация использования искусственного интеллекта в образовательном процессе // Международный журнал гуманитарных и естественных наук. 2023. №4–1 (79).

16. Яо Ли Использование технологии «дипфейк» в Китае: проблемы правового регулирования и пути их решения // Lex Russica. 2024. №11 (216).