КИБЕРТЕРРОРИЗМ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПОТЕНЦИАЛЬНЫЕ РИСКИ И ЭТИЧЕСКИЕ ВОПРОСЫ

Ахмедов М.А., *студент группы СГН3-31Б*
Московский государственный технический университет им. Н.Э. Баумана

Научный руководитель: ***Бочарников И.В.****, доктор политических наук, профессор кафедры «Информационная аналитика и политические технологии»*
nic.bezopasnost@yandex.ru

Аннотация: В статье рассматриваются взаимосвязи между кибертерроризмом и искусственным интеллектом (ИИ). Анализируются потенциальные риски, связанные с использованием ИИ в контексте кибертеррористических актов, а также этические вопросы, возникающие в результате данного взаимодействия. Исследование подчеркивает необходимость разработки норм и стандартов для минимизации угроз и обеспечения безопасности.

Ключевые слова: информация, информационные технологии, кибертерроризм, искусственный интеллект, нейронные сети, машинное обучение, этические вопросы, ответственность, кибератаки, автономные системы.

Кибертерроризм представляет собой одну из наиболее значительных угроз в современном цифровом мире, так как он затрагивает не только отдельные организации, но и целые государства и общества. С развитием информационных технологий и их внедрением в различные сферы жизни – от здравоохранения и энергетики до финансовых и транспортных систем – кибертеррористы получают доступ к новым инструментам и методам, которые могут быть использованы для нанесения ущерба.

На сегодняшний день, ни Уголовный кодекс Российской Федерации [1], ни Федеральный закон «О противодействии терроризму» не формулирует определение понятия «кибертерроризм» [3]. По своей сути, кибертерроризм является преступным деянием, совершаемым в информационной сфере, вследствие чего данное преступление должно быть квалифицировано по статьям из главы 28 УК РФ.

При этом терроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения или иными формами противоправных насильственных действий. Именно поэтому его квалификация должна происходить по соответствующим статьям главы 24 УК РФ.

Таким образом, кибертерроризм – использование компьютерных технологий для террористических актов, создающих хаос и влияющих

на политические решения. Оно может включать в себя, например, атаки на компьютерные системы, сети, а также инфраструктуру, с какой-либо целью, в том числе и политической [12].

Кибертеррористы используют интернет-ресурсы, мессенджеры, СМИ, беспилотные летательные аппараты (БПЛА), мобильные средства связи и многое другое.

Суть тактики кибертерроризма в том, что преступление должно стать широко известным населению, шокировать общество и создать атмосферу угрозы совершения террористического акта в любом месте, в любое время.

Искусственный интеллект (ИИ), в свою очередь, становится мощным инструментом, способным как помочь в борьбе с киберугрозами, так и создать новые риски. С одной стороны, ИИ может использоваться для анализа больших объемов данных, выявления аномалий и предсказания потенциальных угроз. Он может автоматизировать процессы обнаружения и реагирования на инциденты, что значительно может увеличить эффективность киберзащиты. С другой стороны, ИИ также может быть использован кибертеррористами для повышения эффективности своих атак.

В Национальной стратегии развития ИИ до 2030 г., утвержденной Указом Президента Российской Федерации (Стратегия) от 10 октября 2019 года. Согласно статье 5 этого документа, искусственный интеллект (ИИ) определяется, как совокупность технологических решений, способных имитировать когнитивные функции человека и достигать результатов, как минимум сопоставимых с человеческим интеллектом, что также включает в себя способность к самообучению и поиску решений без заранее заданных алгоритмов [2]. Данные технологии используются, например, для анализа больших объемов данных, выявления закономерностей и автоматизации процессов.

Гуманное использование информационных технологий давно волнует человечество. В 1942 году Айзек Азимов в рассказе «Хоровод» впервые сформулировал три закона робототехники:

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинен вред.
2. Робот должен повиноваться всем приказам, которые дает человек, кроме тех случаев, когда эти приказы противоречат Первому Закону.
3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Закону.

С появлением ИИ, по словам Френка Паскуале, три закона А. Азимова необходимо дополнить:

4. Цифровые технологии должны дополнять деятельность профессионалов, а не заменять их.

5. ИИ и роботизированные системы не должны подделывать человека.

6. В области ИИ следует предотвратить усиление гонки вооружения.

7. Роботы и системы ИИ должны указывать на личность своих создателей, контролирующих их людей и владельцев [11].

Однако, на практике поднимается множество этических вопросов, связанных с применением искусственного интеллекта в преступной деятельности, в том числе и в кибертерроризме.

Во-первых, ИИ и машинное обучение могут быть использованы как для защиты, так и для атак. Например, искусственный интеллект может анализировать данные для предсказания и предотвращения кибератак, автоматически устранять уязвимости в системах или помогать в расследованиях [6]. С другой стороны, те же технологии могут быть использованы злоумышленниками для разработки более сложных и эффективных методов атак, таких как создание фальшивых новостей, манипуляции над общественным мнением, или даже автономные кибератаки, которые будут действовать на основе самообучающихся алгоритмов, затрудняя отслеживание источников угроз.

Примером может служить использование нейронных сетей для создания фальшивых видеозаписей или аудиофайлов (deepfake), которые могут быть использованы для кибертеррористических целей – например, для ложных заявлений от имени высокопоставленных лиц с целью посеять панику или повлиять на политические решения. Это явление уже начинает набирать популярность среди мошенников, а также может быть использовано в террористических актах для манипуляции общественным мнением.

Во-вторых, важно понимать, что использование ИИ в террористических целях может привести к новым типам угроз. Например, БПЛА, оснащенные ИИ, могут быть использованы для реализации точечных атак, не требующих участия человека, что осложняет как предупреждение таких атак, так и установление ответственности за их совершение [5]. Вопрос контроля над такими системами, их подотчетности и предсказуемости работы становится одним из самых обсуждаемых в сфере международной безопасности.

В-третьих, нужно обратить внимание на влияние самого обучения ИИ на киберзащиту. Хотя ИИ может помогать в создании эффективных защитных систем, сам процесс обучения алгоритмов может быть использован злоумышленниками для создания алгоритмов, способных обходить эти же защитные меры [8]. Например, ИИ может быть использован для проведения атак «нулевого дня», когда уязвимость была выявлена, но еще не успела получить необходимую доработку. Более того, ИИ, обуча-

ясь на ранее успешных атаках, может быстро адаптироваться и совершенствоваться, создавая новые формы угроз, которые могут быть крайне трудными для предсказания.

В дополнение к вышеупомянутым аспектам, важной проблемой, связанной с кибертерроризмом, использующим ИИ, является определение ответственного лица за совершенные преступления. Например, когда атака осуществляется с помощью автономных систем, таких как дрон с ИИ или алгоритмы, способные самостоятельно принимать решения, возникает сложная юридическая и этическая дилемма [8]. Кто несет ответственность за действия таких систем: разработчики, пользователи, или сама система, которая приняла решение о проведении атаки?

Сложность усугубляется тем, что автономные системы могут действовать без контроля человека, принимая решения на основе алгоритмов и данных, которые они анализируют. Это создает ситуацию, в которой трудно установить прямую связь между конкретным человеком и действиями машины. Например, если дрон, управляемый ИИ, совершает удар по гражданскому объекту, возникает вопрос: следует ли привлекать к ответственности разработчиков ПО, операторов, которые его запустили, или саму технологию?

Кроме того, различные юрисдикции могут иметь разные подходы к определению ответственности в подобных ситуациях. Это создает правовые пробелы и затрудняет международное сотрудничество в борьбе с кибертерроризмом. В результате, отсутствие четких норм и стандартов может привести к безнаказанности злоумышленников, использующих ИИ для проведения атак, что ставит под угрозу безопасность и стабильность как отдельных стран, так и международного сообщества в целом.

Необходимы дальнейшие исследования и разработка норм для минимизации рисков, связанных с использованием ИИ в контексте кибертерроризма. Например, следующие инициативы могут помочь в решении данной проблемы:

- Создание юридического определения для понятия «кибертерроризм» в контексте Уголовного кодекса или Федерального закона поможет установить правовые рамки для борьбы с кибертерроризмом и привлечения к ответственности за преступления, связанные с использованием ИИ.
- Разработка международных соглашений и стандартов, которые будут регулировать использование ИИ в контексте кибербезопасности. Они могут включать в себя сотрудничество между государствами, обмен информацией, совместные усилия по разработке технологий защиты.

- Разработка этических норм для использования ИИ, которые будут регламентировать возможные последствия своих действий для разработчиков и пользователей.
- Обучение и тренинги специалистов в области кибербезопасности, правоохранительных органов и других заинтересованных сторон о потенциальных рисках, связанных с использованием ИИ.
- Сотрудничество государственных органов с частными компаниями, работающими в области ИТ и кибербезопасности, для обмена опытом и разработки совместных решений по борьбе с кибертерроризмом.

В свете обсуждаемых в статье проблем становится очевидным, что эффективная борьба с кибертерроризмом требует не только технологических инноваций, но и нового подхода в законодательной, этической и образовательной сферах. Это особенно важно в условиях, когда злоумышленники могут использовать такой мощный инструмент, как искусственный интеллект. Необходимо, чтобы государства, международные организации и частные компании объединились в усилиях по созданию безопасного цифрового пространства, где ИИ будет служить исключительно на благо человечества, а не в ущерб ему.

Литература и источники:

1. Уголовный кодекс Российской Федерации [Электронный ресурс]: ФЗ РФ от 13 июня 1996 г. № 63-ФЗ: (ред. от 30 дек. 2020 г.) // КонсультантПлюс.

2. Указ Президента РФ от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации.

3. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». http:/ www.consultant.ru.

4. Бочарников И.В., Овсянникова О.А. Риски и вызовы информационной работы при проведении специальных военных и полицейских операций // Вестник Академии военных наук. 20224. № 1. С. 22–29.

5. Бояринов Е. Искусственный интеллект в беспилотных летательных аппаратах. https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-bespilotnyh-letatelnyh-apparatah.

6. Гедгафов М.М. Роль искусственного интеллекта в противодействии терроризму 2023 // URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-protivodeystvii-terrorizmu.

7. Информационная аналитика в современном социально-политическом процессе: теория и практика / Ремарчук В.Н., Бочарников И.В., Артемьев А.А.,

Галаганова С.Г., Гришнова Е.Е., Егоров В.Г., Карась Р.А., Катков О.Н., Ламинина О.Г., Смульский С.В., Шевчун В.Н., Урсул В.И. Москва, 2024.

8. Мохат П.М. Проблемы определения юридической ответственности за действия искусственного интеллекта. https://cyberleninka.ru/article/n/problemy-opredeleniya-yuridicheskoy-otvetstvennosti-za-deystviya-iskusstvennogo-intellekta.

9. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность. https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost.

10. Ремарчук В.Н. Управление смыслами как инструмент современной политики: технологии, вероятные последствия // Этносоциум и межнациональная культура. 2019. № 2 (128). С. 9–21.

11. Паскуале Ф. Новые законы робототехники: апология человеческих знаний в эпоху искусственного интеллекта. – М.: Дело, 2022.

12. Тарасова Л.Я. Эволюция понятия информационного терроризма (кибертерроризма) и его значение на современном этапе. https://cyberleninka.ru/article/n/evolyutsiya-ponyatiya-informatsionnogo-terrorizma-kiberterrorizma-i-ego-znachenie-na-sovremennom-etape.

13. Украинский кризис в условиях трансформации современного миропорядка: тенденции развития, угрозы и вызовы для России / Баранов В.П., Бартош А.А., Бочарников И.В., Дульнев П.А., Караваев И.Н., Кардаш И.Л., Карпович О.Г., Корабельников А.А., Кулаков А.А., Манойло А.В., Овсянникова О.А., Петренко А.И., Ремарчук В.Н., Стригунов К.С., Сурма И.В., Суханов П.В. (2-е издание, исправленное) Москва, 2022.