УДК 004.056

Кибервойна и использование искусственного интеллекта: роль международного сообщества в обеспечении безопасности

Ван Бинъюй

Магистрант,
Московский государственный университет им. М.В. Ломоносова,
119234, Российская Федерация, Москва, Ленинские Горы, 1;
e-mail: wby1402469439@163.com

Аннотация

В данной работе выявляется содержание кибервойны в международном масштабе и эффективность различных методов, используемых для обеспечения безопасности. Автор исследует роль международного сообщества в борьбе с кибертерроризмом, экстремизмом и различными видами кибератак. В работе актуализируются явные и латентные угрозы при кибервойне, а также возможности противостояния им. Основным инструментом, который эффективно используется в международной кибервойне, автор определяет искусственный интеллект – различные его модификации и сферы применения.

В связи с этим основной целью работы определено изучение использования международным сообществом киберинтеллекта в обеспечении безопасности при кибервойне. Объектом является международная кибербезопасность, предметом- использование искусственного интеллекта. На заключительном этапе исследования автор предлагает рекомендации для специалистов, обеспечивающих информационную безопасность, а также для тех, кто косвенно связан с получением, хранением и использованием данных, а также с работой в киберпространстве.

Для цитирования в научных исследованиях

Ван Бинъюй. Кибервойна и использование искусственного интеллекта: роль международного сообщества в обеспечении безопасности // Теории и проблемы политических исследований. 2024. Том 13. № 4А. С. 72-79.

Ключевые слова

Искусственный интеллект, кибервойна, международная безопасность, киберпространство, информационная война, информационная угроза, киберличность.

Введение

Актуальность тематики исследования обусловлена стремительной динамикой развития цифрового сообщества в международном масштабе, нарушениями границ безопасности и появлением такого понятия как «кибервойна», которое функционирует в информационном интернет- пространстве.

Современные войны отражают тенденции развития социума, переходят из реального пространства с вооруженными конфликтами в информационное киберпространство и являются инструментом воздействия не только на физическое, но и на психологическое здоровье населения. Кибервойны имеют множество явных и скрытых угроз, которые реализуются как в интернет- пространстве, так и в реальной жизни. Одна из наиболее главных опасностей данного вида войны заключается в том, что вредоносная информация небезопасна для всех категорий населения, воздействует на сознание и психику людей, особенно подрастающего поколения.

В контексте специальных агрессивных военизированных действий, а также действий преступного, экстремистского и террористического характера важно говорить нарушении государственной, и даже национальной безопасности. В данных случаях происходит взлом программного обеспечения, представляющий угрозу для безопасности не только отдельных групп социума, но и для государства в целом.

Учитывая вышесказанное, необходимо найти эффективные инструменты, позволяющие осуществлять противостояние кибервойне, применять инновационные цифровые технологии, такие, к примеру искусственный интеллект. Также очень важным является изучение роли международного сообщества в обеспечении государственной и межгосударственной безопасности, потенциал цифровых и интеллектуальных ресурсов, которые помогают минимизировать последствия кибервойны.

В связи с этим основной целью работы конкретизировано изучение использования международным сообществом киберинтеллекта в обеспечении безопасности при кибервойне. Объектом определена международная кибербезопасность, предметом- использование искусственного интеллекта.

Для достижения исследовательской цели нами был поставлен ряд следующих задач:

1. Определение понятия и содержания «кибервойна», а также его проявлений в информационном пространстве;

2. Выявление роли искусственного интеллекта в современной жизни;

3. Изучение эффективности применения искусственного интеллекта международным сообществом при обеспечении государственной безопасности в кибервойне.

Методы и методология

В качестве одного из методов в работе используется теоретико- методологический анализ современных источников литературы, которые освещают различные аспекты, связанные с тематикой исследования: исторический аспект трансформации традиционных войн в киберсражения (Н. А. Балаклеец), специфика кибервойны в информационном пространстве (Р. С. Выходец, К. А. Панцерев, Н. В. Карпиленя и др.), а также изучение применения искусственного интеллекта в кибервойне (В. М. Буренок, С. С. Горохова и пр.).

Кроме того, автор применяет сравнительный анализ различных точек зрения на кибервойну и роль в ней искусственного интеллекта, изучая мнения различных исследователей.

Результаты и их обсуждение

Развитие современного общества является достаточно динамичным и его тенденции захватывают все сферы общественной жизни, включая экономику, политику, а также вооруженные конфликты и войны. Цифровизация, имеющая несомненный положительный эффект, включает множество возможностей, которые зачастую используются далеко не в мирных целях. Информационная преступность, кибервойны, интернетатаки захлестывают общество и представляют максимальную угрозу для его безопасности, т.к. кроме характера массового поражения включают сложное, практически невозможное нахождение и наказание исполнителей.

Понятие и содержание «кибервойна», его проявления в информационном пространстве

В эпоху включения цифровых технологий практически во все сферы жизнедеятельности человека приоритетное значение имеют не традиционные, а кибервойны, которые оказывают существенное влияние на информационную и психологическую сферы деятельности человечества. Современный мир уже не может полноценно функционировать без интернета, средств цифровизации, облачных сервисов, Интернет-ресурсов, сообществ, киберпространства и автоматизированных систем. Как отмечают аналитики Business Insider Intelligent, на конец 2025 года во всем мире будет функционировать 34 миллиарда устройств, которые имеют доступ к интернету. Безусловно, с учетом указанных тенденций многие направления экономики, политики, в том числе, и военные действия трансформируются из традиционного в киберпространство [Харланов, Белый, 2021].

По мере развития человечества войны охватывали все новые сферы. различные пространства, а также зоны воздействия. Объектом военных действий перестали быть только переделы территорий и борьба за власть. В современных войнах основным предметов споров, противоречий и агрессивных действий является информация, возможность воздействия на людей.

Если изначально война, по мнению Н. А. Балаклейца [Балаклеец, 2021], была зависима от территории, природных, климатических условий, вооружения и человеческих ресурсов, то на настоящий момент данные ограничения для кибервойны носят минимальный характер, т.к. все атаки проводятся в интернет- пространстве.

Говоря о пространстве войны, необходимо выделить следующие его компоненты [Балаклеец, 2021]:

- зона для планирования и реализации военных операций;
- возможности для перемещения различных объектов (людей и вооружения) в целях осуществления военных действий;
- объективно значимое, специально созданное пространство в контексте реализации атак и вооруженных действий.

Введение новых пространств для военных действий, как отмечает ряд авторов (Р. С. Выходец, К. А. Панцерев и пр.) обусловлено следующими факторами:

-возможность воздействовать на население государств, идеологический и политический строй, вне зависимости от территориального расположения и границ данных стран;

- повышение эффективности и результативности военных действий в киберпространстве.

Кибервойны давно вышли за пределы реальных территорий, обрисованных границами государств и осуществляются в международном информационном пространстве, которое не имеет видимых границ и объем информации которого практически бесконечен. Кибер- и информационные войны имеют своим назначением психологическое воздействие на противника вне зависимости от национальности, места проживания, социального статуса и иных характеристик, которые обуславливают возможность участия в подобного рода действиях.

Как отмечает бывший командующий ВМС США Стюарт Грин, «кибервойны включают в себя: цифровое противостояние, агрессивные действия в социальных сетях, психологические операции, военный обман и государственную (национальную) безопасность» [Выходец, Панцерев, 2022, с. 141]. Поэтому анализируя состав и содержание кибервойны, необходимо

исследовать ее структуру и основные цели. Кибервойна концентрируется на использовании интернет-технологий, информационного пространства Сети, а также активизации киберугроз для массового поражения противника. Данный вид войны основывается на использовании компьютерных технологий для нанесения ущерба или разрушения другим государствам и поэтому наиболее опасна в контексте воздействия не только на физическое, но и психологическое состояние населения.

Кибервойна отражает явные и латентные длительные угрозы, существующие в интернет-пространстве, вне зависимости от территориального расположения и это определяет особо опасный- международный характер кибервойны (А. С. Капто). Это сложное, многогранное явление Н. Р. Красовская, А. А. Гуляев характеризуют как противоборство обществ, государств, политических и идеологических систем, показывая негативное воздействие на все сферы жизнедеятельности. При этом большинство авторов [Буренок, 2021; Выходец, Панцерев, 2022; Горохова, 2020] определяют кибервойну как часть информационной и поэтому инструменты противодействия должны быть масштабными, эффективными и современными.

Применение искусственного интеллекта международным сообществом при обеспечении государственной безопасности в кибервойне

Переоценить значение ИИ в жизни современного общества сложно, т.к. постепенно он находит применение во всех сферах жизни социума. Искусственый интеллект становится основным помощником в медицине, образовании, науке, строительстве и конечно же, в обеспечении государственной безопасности.

Средства искусственного интеллекта стремительно совершенствуются и способствуют формированию цифрового мышления, универсальных компетенций и умений у современных специалистов. Кроме того, использование ИИ в военно- стратегических целях предусматривает интеграцию знаний специалистов в IT- сфере, а также профессионалов военного дела, что обеспечивает максимальную эффективность разведывательной, превентивной и оборонительной деятельности в киберпространстве.

Так как одними из основных целей войны являются манипуляция сознанием населения, формирование искаженного общественного мнения об определенных событиях и явлениях, методы и средства борьбы в данной войне должны быть соответствующими- адаптированными к киберпространству. Важнейшим инструментом часть исследователей определяет искусственный интеллект как часть данного пространства и естественный компонент управления интернет- сообществами международного масштаба. Одним из несомненных преимуществ искусственного интеллекта (ИИ) является его стремительное развитие, возможность адаптироваться к изменяющимся условиям киберпространства. В данном случае речь идет не только о возможностях искусственного разума в области сбора, обработки и использования разведданных, организации логистических перевозок, кибероперациий, военной стратегии и тактики командования и управления. Здесь необходимо говорить еще и об обеспечении работы беспилотных разведывательных и оборонных технологий, функционировании полуавтономных и автономных транспортных средств.

Как подтверждает в своей работе С. С. Горохова [Горохова, 2020] ИИ в недалеком будущем можно будет считать ключевой технологией в реализации военных кибероперациий. Это подтверждено тем, что на одном из выступлений в сенатском комитете по вооруженным силам США адмирал Майкл Роджерс сделал заявление, что самая проигрышная стратегия в информационной войне- это надежда на использование лишь человеческого интеллекта в международном киберпространстве.

Россия также придерживается подобной точки зрения, подчеркивая, что современный уровень угроз кибербезопасности обуславливает использование искусственного интеллекта если не в качестве основного, то вспомогательного средства в противодействии военным информационным атакам.

Несмотря на то, что искусственный интеллект уже широко используется в военных целях, локальных боевых операциях [Горохова, 2020], актуально выявить его эффективность в борьбе с киберагрессорами и обеспечении международной безопасности. Важно подчеркнуть именно объединение стран в международное сообщество в целях борьбы с мировыми проявлениями кибератак и кибервойн. По отдельности государствам достаточно сложно противостоять кибервойне, разрабатывать и использовать программное обеспечение для функционирования искусственного интеллекта.

Говоря об использовании искусственного интеллекта в противодействии кибервойне, необходимо разграничивать уровни ИИ:

-простой уровень использования данного инструментария позволяет автоматизировать процесс сбора, хранения, анализа и использования тактических и стратегических данных, имеющих значение для обеспечения безопасности. В данном случае ИИ может полностью заменить человеческую деятельность и является основой для дальнейшей работы специалистов в области компьютерных технологий и военного дела;

-сложный уровень, который способствует принятию управленческих, командных решений, разработке интеллектуальных программ кибератакам и кибервойнам. Подобное использование ИИ эффективно в сочетании с деятельностью высококлассных специалистов IT-сферы, профессионалов в области военной стратегии и тактики, которые анализируют решения, принятые ИИ и осуществляют дальнейшие действия по обеспечению безопасности.

Направления использования искусственного интеллекта в противодействии кибервойне можно дифференцировать на несколько групп:

1. Разработка международных проектов и программ, ориентированных на обеспечение безопасности при военных действиях традиционного и кибер- характера.

В отношении международной кибербезопасности еще в 2018 г. компания Raytheon предложила специальную систему реагирования на общественные угрозы и их предотвращения в интернет- пространстве «PREVENT». Данная система искусственного интеллекта вычисляет и оценивает объем и модели интернет- траффика, сепарируя особо опасные, террористические и экстремистские контенты. Это позволяет выявлять поставщиков данной информации, анализировать их деятельность, цели и предотвращать атаки на определенные сферы национальной безопасности.

Проект Maven, датирующийся примерно тем же периодом, призван перерабатывать огромный массив информации в международном масштабе, автоматизировать сбор и обработку разведданных, и передача их военным аналитикам, которые будут максимально эффективно использовать полученные сведения.

В данном направлении мировое сообщество активно использует системы компьютерного зрения и автоматизированного сбора разведданных, которые возможно проанализировать с беспилотных воздушных и наземных аппаратов. Это позволит автоматически определять враждебную активность на различных интернет-ресурсах, контентах для конкретного, точечного противодействия.

2. Обеспечение функционирования, обновления и эффективного использования беспилотных аппаратов, полуавтоматических и автоматических транспортных средств, которые

подключены к системе Интернет и могут использоваться как в реальных, так и в кибервойнах, выявляя противников как на территории государств, так и в информационном международном поле.

Спецификой подобных устройств можно определить то, что изначально разработанные для реальных боевых действий, они могут быть использованы и для сбора данных в киберпространстве с перспективой применения этих сведений в обеспечении информационной и военной безопасности государств. Эффективны в работе израильские разработки Elbit, IMI Systems, российские «Форпост», «Альтиус-У» и пр.

В области международного сотрудничества еще с 2012 года работают множество компаний и агентств по использованию цифровых технологий в борьбе с кибервойнами. В пример можно привести американское агентство «Defense Advanced Research Project Agency», российский Фонд перспективных исследований, которые реализуют международные проекты по обеспечению кибербезопасности «Искусственный интеллект и нейротехнологии», «Эра» и ряд других.

Однако, международным сообществом выявляется ряд проблем в противостоянии кибервойне. В частности, можно определить следующее:

1.Невозможность некоторым государствам полноценно обеспечить киберзащиту национальной безопасности в силу дороговизны оборудования, программного обеспечения средств ИИ;

2. Не всегда имеется возможность у стран различных коалиций договориться в стратегических вопросах ведения кибервойны и результатом этого является диссонанс и противоречия в реализации программ и проектов;

3. Функционирование агрессирующих сторон с более совершенным оборудованием и программным обеспечением, чем системы государственной защиты не позволяет своевременно выявлять и пресекать попытки кибератак.

Заключение

В заключение нашего исследования необходимо отметить актуальность изучения использования международным сообществом средств искусственного интеллекта в противостоянии кибервойне.

Поставленные на начальном этапе задачи, были решены:

1.Определено понятие и содержание термина «кибервойна», а также его проявления в информационном пространстве, которые заключаются в совершении агрессивных и деструктивны действий, направленных на разрушение либо ущерб конкретным государствам, либо группам социума.

2.Выявлена роль искусственного интеллекта в современной жизни, отражающая вспомогательные функции для оптимизации и автоматизации деятельности различных интеллектуальных уровней;

3. Изучена эффективность применения искусственного интеллекта международным сообществом при обеспечении государственной безопасности в кибервойне. Данный инструментарий предполагает объединение государств в борьбе с кибератаками, экстремизмом и терроризмом, а также постоянное обновление и совершенствование средств ИИ.

Обозначенные в работе проблемы возможно разрешить только при комплексном подходе, развитии сети международных организаций, обеспечивающих кибербезопасность в

межгосударственном пространстве. При этом важно понимать, что те, кто осуществляет агрессию в информационном пространстве, имеют современные цифровые ресурсы и средства ИИ для максимально негативного воздействия на большую часть населения. Поэтому важно наносить превентивные удары, выявление и предотвращение попыток осуществления киберугроз и делать это регулярно и слаженно.

Библиография

1. Балаклеец Н. А. Пространственный аспект современных войн: от традиционной войны к кибервойне // Социодинамика. 2021. №4. С. 136-149.
2. Буренок В. М. Искусственный интеллект в военном противостоянии будущего // Военная мысль. 2021. №4. С. 106-112.
3. Выходец Р. С., Панцерев К. А. Сравнительный анализ современных концепций информационного противоборства // Евразийская интеграция: экономика, право, политика. 2022. №4 (42). С. 139-148.
4. Горохова С. С. Искусственный интеллект в контексте обеспечения национальной безопасности // Национальная безопасность / nota bene. 2020. №3. С. 15-31.
5. Карпиленя Н. В. О диалектике войны в контексте современных типов информационных «войн» и методов информационно-психологического противоборства // Архонт. 2022. №1. С. 29-42.
6. Красовская Н. Р., Гуляев А. А. К вопросу классификации информационных войн // Социология науки и технологий. 2019. №2. С. 44-55.
7. Кузнецов Д. И. Цифровая эпоха и новые подходы к глобальной безопасности // Россия в глобальном мире. 2022. №23 (46). С. 142-152.
8. Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. №2. С. 2-8.
9. Подопригора А. В. Искусственный интеллект как дискурс самопознания и самоорганизации цифрового социума // Социум и власть. 2019. №1 (75). С. 7-20
10. Харланов А. С., Белый Р. В. Новые реалии ведения войны: «кибертерроризм» и информационные войны // Юридическая наука. 2021. №6. С. 106-110.

Cyberwarfare and the use of artificial intelligence: the role of the international community in ensuring security

Wang Bingyu

Master student,
Lomonosov Moscow State University,
119234, 1, Leninskie Gory, Moscow, Russian Federation;
e-mail: wby1402469439@163.com

Abstract

This paper identifies the content of cyber warfare on an international scale and the effectiveness of various methods used to ensure security. The author explores the role of the international community in the fight against cyberterrorism, extremism and various types of cyber attacks. The paper actualizes explicit and latent threats in cyberwarfare, as well as the possibilities of countering them.

The author defines artificial intelligence as the main tool that is effectively used in international cyber warfare – its various modifications and applications.

In this regard, the main purpose of the work is to study the use of cyberintelligence by the international community in ensuring security during cyberwar. The object is international cybersecurity, the subject is the use of artificial intelligence.

At the final stage of the study, the author offers recommendations for specialists who ensure information security, as well as for those who are indirectly involved in obtaining, storing and using data, as well as working in cyberspace.

For citation

Wang Bingyu (2024) Kibervoina i ispol'zovanie iskusstvennogo intellekta: rol' mezhdunarodnogo soobshchestva v obespechenii bezopasnosti [Cyberwarfare and the use of artificial intelligence: the role of the international community in ensuring security]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 13 (4A), pp. 72-79.

Keywords

Artificial intelligence, cyberwarfare, international security, cyberspace, information warfare, information threat, cyber personality.

References

1. Balakleets, N. A. (2021). The spatial aspect of modern wars: From traditional warfare to cyber warfare. Sociodynamics, 4, 136–149.
2. Burenok, V. M. (2021). Artificial intelligence in the military confrontation of the future. Military Thought, 4, 106–112.
3. Vykhodets, R. S., & Panzeriev, K. A. (2022). Comparative analysis of modern concepts of information confrontation. Eurasian Integration: Economics, Law, Politics, 4(42), 139–148.
4. Gorokhova, S. S. (2020). Artificial intelligence in the context of national security provision. National Security / Nota Bene, 3, 15–31.
5. Karpilenya, N. V. (2022). On the dialectics of war in the context of modern types of information "wars" and methods of information-psychological confrontation. Archont, 1, 29–42.
6. Krasovskaya, N. R., & Gulyaev, A. A. (2019). On the classification of information wars. Sociology of Science and Technology, 2, 44–55.
7. Kuznetsov, D. I. (2022). The digital age and new approaches to global security. Russia in the Global World, 23(46), 142–152.
8. Lebed, S. V. (2022). Innovative technologies in the field of cybersecurity. Modern Information Technologies and IT Education, 2, 2–8.
9. Podoprihora, A. V. (2019). Artificial intelligence as a discourse of self-knowledge and self-organization of the digital society. Society and Power, 1(75), 7–20.
10. Kharlanov, A. S., & Belyi, R. V. (2021). New realities of warfare: "Cyberterrorism" and information wars. Legal Science, 6, 106–110.