

2. Anckar D. Direct democracy in microstates and small island states // *World Development*. – 2004. – Т. 32. – №. 2. – С. 379-390.
3. Esaiasson P. Gilljam, Mikael. Oscarsson, Henrik. Wängnerud, Lena // *Metodpraktikan: konsten att studera samhälle, individ och marknad*. – 2007.
4. Huntington S. P. How countries democratize // *Political science quarterly*. – 2021. – Т. 106. – №. 4. – С. 579-616.
5. Khan A. A. et al. The role social of media and modern technology in arabs spring // *Far East Journal of Psychology and Business*. – 2012. – Т. 7. – №. 1. – С. 56-63.
6. Rustow D.A. 2. Transitions to Democracy: Toward a Dynamic Model // *Transitions to democracy*. – Columbia University Press, 2020. – С.14-41.
7. Sarhan A. Is the Arab Spring in the Third Wave of Democratization? The Case of Syria and Egypt // *Turkish Journal of Politics*. – 2019. – Т. 3. – №. 1.
8. Skocpol T., Theda S. States and social revolutions: A comparative analysis of France, Russia and China. – Cambridge University Press, 2019.
9. The Economist, 2011. "The Long standoff: The shoe-thrower's index". The Economist. 2011-02-11.

МРНТИ 11.15.69

<https://doi.org/10.51889/2959-6270.2023.82.2.006>

Рау И.А.,^{1*} Абсамтаров Р.Б.²

¹ Академия ведущих кадров Бундесфера
г. Гамбург, Германия,

² Казахский национальный педагогический университет им. Абая
г. Алматы, Республика Казахстан

ПРЕДУПРЕЖДЕНИЕ ЭЛЕКТРОННЫМИ СИСТЕМАМИ И ЧЕЛОВЕКОМ ЯДЕРНЫХ УГРОЗ: ПОЛИТИЧЕСКО-СОЦИОЛОГИЧЕСКИЙ АНАЛИЗ

Аннотация

В статье рассматриваются проблемы предупреждения электронными системами и человеком ядерных угроз, которые ещё не изучены в социально-политической науке. В статье более подробно рассматриваются вопросы предупреждения электронными системами и человеком ядерных угроз: искусственный интеллект и разум в предотвращении ядерной катастрофы; ненадёжности в системе раннего предупреждения; контекстные знания; предложения по преодолению сомнений; о возможности большой безопасности на основе неполной информации электронных систем; какая из систем контроля внезапного нападения надежнее. В статье отмечается, что наличие ядерного оружия даже у равносильных держав не есть гарантия ядерной катастрофы. Гарантия возможности скорейшего ответного ядерного удара – одно из решающих условий предотвращения ядерной агрессии. Компьютерная система раннего предупреждения и электронные системы по принятию решений нацелены на своевременное определение ядерного нападения.

В мирные времена и в период разрядки напряжённости между ядерными державами риск относительно мал, что компьютерный сигнал о нападении немедленно ведёт к ответному ядерному удару. В такой ситуации резко возрастает роль человека в принятии решения по сомнительному сигналу ядерная атака. Ситуация резко меняется во времена кризисных обострений отношений между ядерными державами вплоть до выражения взаимных угроз.

Ключевые слова: ядерное оружие, ядерная угроза, электронная система, катастрофа, безопасность.

И.А. Рау,^{1*} Р.Б. Әбсаттаров²

¹ Бундесфердің жетекші кадрлардың академиясы
Гамбург қ., Германия,

² Абай атындағы Қазақ ұлттық педагогикалық университеті
Алматы қ., Қазақстан Республикасы

ЭЛЕКТРОНДЫҚ ЖҮЙЕЛЕР ЖӘНЕ АДАМНЫҢ ЯДРОЛЫҚ ҚАТЕРЛЕРДІҢ АЛДЫН АЛУЫ: САЯСИ-ӘЛЕУМЕТТАНУЛЫҚ ТАЛДАУ

Аннотация

Мақалада электронды жүйелер мен адамның әлеуметтік-саяси ғылымда әлі зерттелмеген ядролық қауіптердің алдын алу мәселелері қарастырылады. Мақалада электронды жүйелер мен адамның ядролық қауіптердің алдын алу мәселелері толығырақ қарастырылады: ядролық апаттың алдын алудағы жасанды интеллект пен ақыл; ерте ескерту жүйесіндегі сенімсіздік; контексттік білім; күмәнді жеңу бойынша ұсыныстар; электрондық жүйелердің толық емес акпаратына негізделген үлкен қауіпсіздік мүмкіндігі туралы; кенеттен шабуылды бақылау жүйелерінің қайсысы сенімдірек. Мақалада ядролық қарудың болуы, тіпті баламалы державалардың да ядролық апатқа кепілдік бермейтіні атап өтілген. Жаңа ядролық соққының ертерек жауап беру мүмкіндігінің кепілі – ядролық агрессияның алдын алудың шешуші шарттарының бірі. Компьютерлік ерте ескерту жүйесі және электронды шешім қабылдау жүйелері ядролық шабуылды уақтылы анықтауға бағытталған. Бейбіт уақытта және ядролық державалар арасындағы шиеленісті бәсеңдету кезеңінде қауіп салыстырмалы түрде аз, бұл шабуыл туралы компьютерлік сигнал бірден ядролық соққыға әкеледі. Мұндай жағдайда адамның күмәнді сигнал бойынша шешім қабылдаудағы рөлі күрт артады ядролық шабуыл. Ядролық державалар арасындағы қарым-қатынастың дағдарыстық шиеленісуі кезінде, өзара қауіп-қатердің көрінісіне дейін жағдай күрт өзгереді.

Түйін сөздер: ядролық қару, ядролық қауіп, электронды жүйе, апат, қауіпсіздік.

I.Rau^{1*}, R.Absattarov²

¹ Academy leading personnel of the Bundesfer,
Hamburg, Germany

² Kazakh National Pedagogical University named after Abai
Almaty, Republic of Kazakhstan

ELECTRONIC SYSTEMS AND HUMAN PREVENTION OF NUCLEAR THREATS: POLITICAL AND SOCIOLOGICAL ANALYSIS

Annotation

The article deals with the problems of preventing nuclear threats by electronic systems and humans, which have not yet been studied in socio-political science. The article discusses in more detail the issues of prevention of nuclear threats by electronic systems and humans: artificial intelligence and intelligence in preventing a nuclear catastrophe; unreliability in the early warning system; contextual knowledge; suggestions for overcoming doubts; about the possibility of greater security based on incomplete information of electronic systems; which of the surprise attack control systems is more reliable. The article notes that the presence of nuclear weapons even among equivalent powers is not a guarantee of a nuclear catastrophe. The guarantee of the possibility of a new nuclear strike as soon as possible is one of the decisive conditions for preventing nuclear aggression. The computer early warning system and electronic decision-making systems are aimed at timely detection of a nuclear attack.

In times of peace and during the period of defusing tensions between nuclear powers, the risk is relatively small that a computer signal of an attack immediately leads to a retaliatory nuclear strike. In such a situation, the role of a person in making a decision on a dubious nuclear attack signal increases dramatically. The situation changes dramatically in times of crisis exacerbations of relations between nuclear Powers, up to the expression of mutual threats.

Keywords: nuclear weapons, nuclear threat, electronic system, catastrophe, security.

ВВЕДЕНИЕ

Ядерное оружие и наличие реальных средств его доставки к цели рассматривается всеми странами, не только ядерными державами, как средство сдерживания от нападения более сильного врага. К приобретению такого оружия стремятся все государства, не входящие в военно-политические блоки и стремящиеся сохранить свою независимость.

Наличие ядерного оружия даже у равносильных держав не есть гарантия ядерной катастрофы: ошибки в оценках намерений друг другу, интерпретация сигналов систем информации, ошибки в интуиционных оценках возможных угроз и др. Эти ошибки смертельно опасны для существования человечества особенно в кризисные ситуации, каковую и мы переживаем (октябрь 2022). Во время Кубинского кризиса и в период всей холодной войны имелся ряд ситуаций, когда от ядерной катастрофы человечество спасал случай, а не данные компьютерных систем предупреждения или интуиция отдельных участников событий. С осознанием гибельности ядерной войны для всех в годы холодной войны был заключен ряд международных договоров по ограничению и по нераспространению ядерного оружия (Договор о неприменении ядерного оружия; NEW Start или INF\$ I – Договор, Intermediate Range Nuclear Forces и др.). Такие договоры и соглашения неоднократно недовыполнялись или просто нарушались со стороны США и НАТО под благовидными предложениями, а на деле – с целью получения ядерного преимущества. Ограничительные договоры не остановили ни противоборство двух социальных систем, ни гонки вооружений, ни совершенствования отдельных видов вооружений, контроль за попытками применения которых становился все более сложным и ненадежным. За короткое время появились новые носители ядерных зарядов, способные доставить их со сверхзвуковой скоростью на любую точку территории противника; оружие стало проникать в космос; возникли многие виды и способы электронного противостояния; широко начали применяться системы искусственного интеллекта; появились системы вооружений, действующие автономно; продолжают качественно создаваться сами ядерные заряды. Все это происходит на фоне стремительного, крайне опасного для мира обострения отношений между США и Россией, НАТО и Россией [1].

Следует сказать, что вопросы предупреждения электронными системами и человеком ядерных угроз ещё не изучены в социально-политической науке. Мы в статье рассмотрим только некоторые социально-политические проблемы предупреждения электронными системами и человеком ядерных угроз.

Цель статьи является политическо- социологический анализ проблемы предупреждения электронными системами и человеком ядерных угроз в мире. Исходя из цели исследования, нами намечены следующие задачи: изучить искусственный интеллект и разум в предотвращении ядерной катастрофы; выявить надёжности в системе раннего предупреждения ядерной угрозы; раскрыть контекстные знания; рассмотреть о возможности большей безопасности на основе неполноценной информации электронных систем; определить какая из систем контроля внезапного нападения надёжнее.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

Методологической основой исследования послужили фундаментальные положения философии, политологии, социологии, военной истории, достижения мировой общественно-политической мысли по проблемам ядерных войн и угроз. В случае предупреждения электронными системами и человеком ядерных угроз, методология может включать разные методы. Анализ статистических данных является важным методологическим подходом для выявления тенденций и закономерностей в предупреждении и реагировании на ядерные угрозы. Этот подход позволяет использовать количественные данные для выявления статистически значимых связей и паттернов в событиях, связанных с ядерной безопасностью. Метод, который может использоваться для выявления внутренних нарушителей, - это наблюдение во время работы, проводимое с целью проверки возможного осуществления несанкционированных действий. Цели наблюдения состоят в обеспечении уверенности в том, что деятельности любого уполномоченного сотрудника всегда контролируется по меньшей мере еще одним опытным, уполномоченным сотрудником, с тем чтобы несанкционированные действия одного из них могли быть немедленно обнаружены и доведены до сведения тех, кого это касается (применяется «правило двух лиц»). Этот метод обнаружения способен обеспечить механизм оперативной выработки и оценки тревожного сигнала. Наблюдение может осуществляться с привлечением для этой цели коллег, руководителей или с помощью кабельного телевидения.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

Искусственный интеллект и разум человека в предотвращении катастрофы

Компьютерные системы раннего предупреждения и электронные системы по принятию решений нацелены на своевременное определение нападения как ядерного. Следующая функция подобных систем – определение совокупности условий, позволяющих нанести немедленный ответный удар по источнику нападения, которого точно определить становится все труднее. И весь процесс идет в автоматическом режиме, вовсе не исключаящем, как полагают некоторые оптимисты, ошибок.

Время прилета ракет после обнаружения составляет пару минут и становится короче (сверхзвуковые ракетные системы становятся еще более скоростными). Увеличивается количественно и качественно число искусственных космических объектов с не вполне известным назначением. Перечисленные факторы, если мы осознаем ограниченность органов восприятия человека относительно скорости изменения указанных выше факторов. Поэтому использование искусственного интеллекта (КИ) в этой сфере деятельности, как и во многих других, неизбежно. Существенные недостатки искусственного интеллекта – отсутствие эмпатии и интуиции. Гарантия возможности скорейшего ответа нового ядерного удара – одно из решающих условий предотвращения ядерной агрессии. Ответный удар требует, пусть малого, но времени и достаточный потенциал. Универсальная формула для такой ситуации: «Кто стреляет первым, тот умирает вторым».

Сегодня признано невозможным создание электронной системы обнаружения ядерного нападения, которая была бы лишена возможности ошибиться. Огромная совокупность данных по обнаружению нападения – источник неопределенных, недостаточных, смутных сведений. Взаимосвязь оценок реальной опасности ядерного нападения с данными компьютерных систем и психическим состоянием личности-контролера несомненна. В годы нарастания напряженности отношений между ведущими ядерными державами возможность ошибок увеличивается. В годы «нормализации» этих отношений – уменьшается.

Чем массивнее и разнообразнее данные электронных систем обнаружения атаки, чем с большей скоростью они изменяются, тем меньше становится возможность человека-контролера вмешаться в принятое машиной решение. Решения систем предупреждения на большом количестве данных, поставляемых многочисленными сенсорами, а также на контекстной информации о возможности вмешательства человека в принятое решение, и о политической ситуации между соперниками и в мире, неопределенность, неполнота, случайность могут привести к военному конфликту.

Естественный язык не вполне пригоден для машинных, электронных систем

Несколько слов о знании надежном – ненадежном и неопределенном, но имеющим вид надежного. Берем случай, когда X является ребенком от У, а этот последний является ребенком от Ц, и тогда X является внуком Ц. Такое правило может быть принято действующим. Выводы, которые делаются на основе этого правила ведут к корректным результатам. Это при том, что корректными были все предпосылки. Аспекты неопределенности и неполноты в таких правилах не учитываются.

Следующий пример показывает ненадежное правило. Если X – это автомашина, а У – это владелец X, то У является одновременно пользователем X. Это правило может считаться правилом, т. к. допускает еще больше исключений, чем пример с внуком, который им может и не быть. Пользователями автомобиля могут быть и дети владельца, равно как и любой человек, имеющий доверенность от владельца.

Пример вопиющей неопределенности. Если X есть тяжелый автомобиль, то X требуется большое количество горючего. Возникают вопросы: что означает «тяжелый», «много»? Но без точного определения этих терминов невозможно говорить об истинности или заблуждении высказываний с этими терминами.

Все положения, допускающие возможность исключений, не могут вести к истине, а лишь к ее подобию, когда речь идет об исключениях и полуисключениях. Пример: если X птица, то X может летать. Но существует множество птиц, которые не могут летать: страус, курица, киви и др. К выводам из таких положений всегда следует относиться с определенной степенью осторожности. Автоматические заключения систем по переработке информации, на основе данных, не достоверных на 100%, требуют в каждом случае дополнительного обоснования. Электронные устройства нуждаются в разъяснениях, пояснениях, касающихся неявных, фоновых знаний и информации, во много в большей степени, чем человек. Но получив точную информацию, такие устройства много быстрее, неустанней, надежней в решении нетворческих задач по сравнению с человеком.

В практической жизни имеется множество взаимосвязей, результат реализации которых непредсказуем, ненадежен и, стало быть, имеют границы применимости. Но в повседневной практической жизни положения, допускающие многие исключения, применимы, а порою и необходимы. Особенно

важны в практической жизни методы заключения по наибольшей вероятности. Для этого рассматриваются, подсчитываются многие вероятности и выбираются наибольшие. Во многих случаях неопределенность и неполнота перерабатываются, что положения могут функционировать как «типичные», «нормальные». То, что птицы могут летать – типично; как и то, что владелец автомобиля является и его пользователем. Пока не обнаружены факты, не вписывающиеся в логику предыдущих положений и не возникает противоречия между общими положениями и фактами.

Подобные противоречия возникают и при создании и функционировании систем искусственного интеллекта (КИ), которые играют решающую роль в системах раннего предупреждения ядерного нападения. Для их разрешения применяются многочисленные и разнообразные логические методы [2].

Ненадежности в системе раннего предупреждения

Ошибки в таких системах могут возникать от редких световых эффектов, идущих от Луны или Солнца, или от стаи птиц, зафиксированных радаром и неверно интерпретированных КИ. Вместе с новыми техническими возможностями растет и количество, и своеобразие сенсоров для более достоверного распознавания ракетного нападения. Стабильно растет количество и разнообразие объектов в воздушном (Дронен и др.) и космическом (спутники и др.). К тому же нарастают проблемы своевременного распознавания сгорающих в земной атмосфере (стратосфере) остатков космического мусора... Это обстоятельство – еще более ненадежных оценок реальности ядерного нападения. При оценке данных системы сенсоров по отношению к сгорающим искусственным объектам сложности могут возникать из-за неопределенностей в яркости и размерах таких объектов. С появлением ракет с управляемой (извне или самостоятельно) системой дополнительно усложняется.

Контекстные знания

В мирные времена и в периоды разрядки напряженности между ядерными державами риск относительно мал, что компьютерный сигнал о нападении немедленно ведет к ответному ядерному удару. В такой ситуации резко возрастает роль человека в принятии решения по сомнительному сигналу ядерной атаки. Ситуация резко меняется во времена кризисных обострений отношений между ядерными державами, вплоть до выражения взаимных угроз.

В марте 2018 г. Министерство обороны ФРГ приняло проект Preview с целью при помощи систем искусственного интеллекта предотвращать кризисы и войны. Ожидания оказались вполне, как показали последующие годы, мечтаниями. На деле предотвратить кризисы и войны могли бы авторитетные руководители противостоящих держав, элиты этих государств, всеобщие антиправительственные восстания в них, но никак не более совершенные электронные системы по предупреждению ядерного нападения сами по себе.

Предложения по преодолению сомнений

В обществе издавна господствует мнение о том, что искусственный интеллект не может давать судьбоносные рекомендации для человечества. Недавно была выпущена в Германии WWW autonomen-waffen.org. Цель этого документа – запрещение автоматических электронных систем препредупреждения, могущие без участия человека вызвать ответный ядерный удар. Это же требование содержится в коалиционном договоре нынешнего трехпартийного правительства (Социалисты, Зеленые и Либеральные демократы – SPD, Grünen und FDP) [3].

Скорость реакции электронных контролеров возможного нападения в миллионны раз превышает скорость принятия решений человеком. Если предварительно не было принято множество решений по реакции на непредвиденные ситуации. Этой очевидности противостоит другая: автоматические системы принятия решений стали повседневностью в обыденной жизни. Эта привычка распространяется и на решения глобального характера.

О возможности большей безопасности на основе неполной информации электронных систем

Насколько доверие к автоматике закрепилось в обыденном сознании, видно из высказываний героев популярного романа Qualityland 2 von Autor Marc Uve Kling. S. 296: «Генрих размышлял: «Уверен ли ты, что третья мировая война может предотвращена решением одного человека?». Следующий вопрос: «Петер подчеркивает, то Все зависит от содержания человека в сравнении с содержанием электронного контролера». Под всеуказанным информационным содержанием предупреждающих информационных систем стоят конкретные люди. Но они не способны вложить в них свой духовно-эмоциональный и моральный мир. Все эти преимущества разумно-духовного существа в предотвращении случайности ядерной катастрофы могут нивелироваться вмешательством политических властей. Вмешательство людей властно-влиятельных, но некомпетентных в решении конкретных проблем почти всегда ведут к негативным последствиям. Человечеству катастрофой в Чернобыле (1986 г.) был дан пример опасности подобного вмешательств «некомпетентных».

ЗАКЛЮЧЕНИЕ

Никто не пытается обвинить автоматические системы в ошибках или в намерениях навредить человеку и миру. Во всех ошибках таких систем и механизмов виноваты их создатели. А они вполне могут иметь намерения навредить.

Если электронные системы предупреждения или отдельные ее части подают сигналы – это не обманки. Обманками бывают интерпретации этих сигналов человеком. Такие интерпретации могут предотвратить ядерную катастрофу, а могут ее и вызвать. Широко известны два примера, подтверждающих сказанное.

Пример 1. В январе 2020 г. в США убили иранского генерала Солеймани при помощи удара с дрона. Иран ответил на это преступление пару дней спустя массированными ударами с воздуха по американским соединениям в Ираке. Через день после этого иранцы по ошибке сбили украинский пассажирский самолет. Иранцы поясняли, что самолет был принят за американский аппарат, несущий ядерный заряд. В ситуации крайней политической напряженности между Ираном и США команда иранских наблюдателей была «склонна» принять мирный самолет за носитель ядерного заряда и нападения. Система электронного наблюдения не имела бы подобной «склонности» и не ошиблась бы в определении объекта. Кроме этого, система электронного контроля имела бы возможность за короткое время проверить план полета иностранных самолетов над Ираном.

Пример 2. Советский спутник раннего предупреждения о ядерном нападении: 23 сентября 1983 года пять межконтинентальных ракет приближаются и подлетают к территории СССР. Получив эту информацию, дежурный офицер Станислав Петров должен был, согласно инструкциям, сообщить об этом немедленно вышестоящей инстанции, чего он не сделал. Петров полагал, что пять межконтинентальных ракет явно нельзя рассматривать как удар по СССР; их не хватило бы даже для ударов по крупным городам страны. К тому же, Петрову было известно о сбитом над нейтральными водами русской ракетой корейском гражданском самолете. Это трагическое событие вызвало резкое возрастание международной напряженности, между США и СССР в особенности. Петров опасался, что сообщение о ложном нападении может вызвать настоящий ядерный ответ СССР. Это «была бы обще-человеческая катастрофа» [4].

В заключение следует сказать, что ядерное оружие – это совокупность ядерных боеприпасов, средств доставки к цели и средств управления, это самое опасное оружие на земле. Применение этого оружия в конфликте или войне гибель для всего человечества. Поэтому предупреждение электронными системами и человеком – контролером ядерных угроз – это возможность предотвратить гибель человечества.

Литература:

1. Bläsius K.H.. *Künstliche Intelligenz und nukleare Bedrohungen*. – B. Budrich Verlag, 2022.
2. Anderson Ross. *Security Engineering*. – New York, 2020.
3. *Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIT GRÜNEN und FDP*. – Berlin 2021. – S.115.
4. Абсаттаров Р.Б., Рау И.А. Отмена договора о ракетах малой и средней дальности. Стремительное ускорение гонки вооружений // Вестник КазНПУ. Серия социологические и политические науки. – 2019, №1. – С. 175.

References:

1. Bläsius K.H. *Künstliche Intelligenz und nukleare Bedrohungen*. – B. Budrich Verlag, 2022.
2. Anderson Ross. *Security Engineering*. – New York, 2020.
3. *Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIT GRÜNEN und FDP*. – Berlin 2021. – S.115.
4. Absattarov R.B., Rau I.A. *Otmena dogovora o raketah maloj i srednej dal'nosti. Stremitel'noe uskorenie gonki vooruzhenij* // Vestnik KazNPU. Seriya sociologicheskie i politicheskie nauki. – 2019, №1. – S. 175.