Интернет военных вещей: концепт, функционально-целевое назначение, структура, регуляторика

И.В. Понкин

Аннотация **– Статья посвящена исследованию роли и значения концепта и технологий *интернета военных вещей* в конкуренции военных потенциалов ведущих держав мира. В статье подчёркнуто, что концепция интернета вещей в целом, в принципе, зародилась в оборонном сообществе, возникла благодаря работе оборонной промышленности над сенсорными сетями и маломощными вычислительными платформами. Автор объясняет концепт интернета вещей, отмечая полную ожидаемость и логичность перехода гражданских технологий интернета вещей в военные приложения. Автор кратко показывает значение интернета военных вещей, придаваемое ему в документах военного стратегического планирования и управления ряда зарубежных государств. В статье обозреваются объяснения сути интернета военных вещей, представленные в научной литературе. В статье представлен развёрнутый авторский концепт объяснения понятия интернета военных вещей и его структуры. В статье рассматривается текущее и потенциально возможное применение технологий интернета вещей в военной сфере. Автор приводит некоторые данные относительно масштабов рынка устройств и систем интернета военных вещей. Автором показаны две существенные особенности применения интернета военных вещей – 1) выраженно враждебный и жёсткий характер среды поля боя и 2) критические ресурсные проблемы, связанные с энергоснабжением, коммуникациями и централизованными облачными вычислительными архитектурами. В статье обозначены ключевые перспективные направления совершенствования систем и комплектующих интернета военных вещей. Сделаны выводы, что отрытого нормативного правового регулирования непосредственно интернета военных вещей нигде не существует; непосредственное регулирование интернета военных вещей сводимо к урегулированию секретными актами государственного управления.**

Ключевые слова **— интернет военных вещей, цифровизация военного управления, технологии двойного назначения, искусственный интеллект, конкуренция военных преимуществ, регуляторные технологии (РегТех).**

I. Введение

Военные технологии всегда были и будут в фокусе военного искусства, и информация всегда была и будет в центре войны. Обмен информацией в режиме реального времени между военными секторами является одним из наиболее важных аспектов военного управления. Растущие технологические способности интегрировать разрозненные системы и подсистемы, сети в большую интегрированную сеть произведёт (и уже производит) революцию в военном деле [1].

В числе новейших технологий военного назначения, оперирующих данными (см.: [2]), отдельное место занимает концепт (и соответствующие технологические решения) так называемого **интернета военных вещей**, функционально «заточенного» под интересы, ожидания, запросы и требования военного управления и другого военного применения.

Интернет военных вещей (англ. – «*Internet of Military Things*» (IoMT)) – это разновидность (таксон в таксономии, класс) и специализированный (под военное назначение) сегмент интернета вещей (англ. – «*Internet of Things*» (IoT)). В качестве синонимов также используются – военный Интернет вещей (англ. – «*Military Internet of Things*» (MIoT)) и Интернет вещей боевого пространства (англ. – «*Battlespace Internet of Things*» (BIoT) или «*Internet of Battlefield Things*» (IoBT)).

Тема интернета военных вещей претерпела всплеск научного и прикладного аналитического интереса в последние 3–5 лет (хотя и не сказать, что публикаций так уж много), но до сих пор не исчерпана, нуждаясь в обобщениях и объяснениях.

И эта тема представляет академический интерес не только для военно-технической науки, но и для гражданского применения, позволяя лучше разобраться в потенциалах приложений интернета вещей в целом.

Тем более, что малоизвестным, но всё же фактом является, что концепция интернета вещей, в принципе, зародилась в оборонном сообществе, возникла благодаря работе оборонной промышленности над сенсорными сетями и маломощными вычислительными платформами. Этот прорыв в использовании Интернета вещей берет своё начало в военных научно-технических проектах [3, с. 1; 4, с. 1].

II. Общее понятие интернета вещей

Интернет вещей основывается на инновационных наработках в области сенсорных сетей и лёгких маломощных вычислительных платформ. Интернет вещей – это междисциплинарная технология, объединяющая сетевые технологии, встроенное оборудование, программные архитектуры, сенсорные технологии, управление информацией, аналитику

Статья получена 20 февраля 2024 г.

И.В. Понкин – Институт государственной службы и управления Российской академии народного хозяйства и государственной службы при Президенте РФ, доктор юридических наук, профессор (e-mail: ponkin-iv@ranepa.ru).

данных и визуализацию. Ключевым моментом Интернета вещей является использование распределённых сетей устройств, которые взаимодействуют через интернет-протоколы и, нередко, через сервис-ориентированные архитектуры. В данном случае «вещью» может выступать любое устройство, для которого может быть функционально применима дистанционная связь, сбор данных или управление. Согласно широкой интерпретации, «вещами» могут быть: транспортные средства, приборы, медицинские и оздоровительные устройства, электрические сети, транспортная инфраструктура, производственное оборудование, системы зданий, иные объекты, наделённые способностями к восприятию и передаче данных. Сенсорные технологии (например, сенсорное зондирование окружающей среды, людей и устройств и др.) так же лежат в основе интернета вещей [3, с. 1].

Согласно нашему концепту, **Интернет вещей** – мета-системный комплекс (со своей функциональной архитектурой) предметов повседневной жизни и / или технологического процесса, оснащённых микропроцессорами-контроллерами и устройствами мониторинга (датчиками), соединённых в сети посредством протоколов и каналов связи, что обеспечивает оперативный обмен данными и оперативную совместимость в целях расширения и комплементарного взаимного достраивания в функционалах и усиления возможностей при совместном применении. В основе интернета вещей – инструментально-технологическая и логистическая цифровая платформа, своего рода **цифровая экосистема.** В интернете вещей данные, собираемые от интегрированных вещей, хранятся, очищаются, интегрируются с данными других систем и аналитически обрабатываются, становясь частью потока данных. Однако подключённые устройства способны и самостоятельно (автоматически) оперативно аналитически обрабатывать и передавать данные, управлять ими.

III. Интернет военных вещей в документах военного стратегирования зарубежных государств

В документах стратегического планирования и управления ключевых акторов НАТО (США, Великобритании, см., например: [5; 6]) и самой организации [7], в их военных подрядах [8] концепту интернета военных вещей придаётся высокое значение (хотя прямое упоминание названия указанного концепта встречается нечасто). Этот концепт всё чаще упоминается в официальных выступлениях высших должностных сил США и Великобритании (см., например: [9]).

В документах некоторых армий мира (например, Австралии) концепт интернета военных вещей отнесён к концепту ускоренной интенсивной войны (англ. – «*accelerated warfare*») (см.: [10]).

IV. К вопросу о понятии интернета военных вещей

Вполне естественно, что технологии интернета вещей переходят в военные приложения, поскольку военные в значительной степени зависят от коммерческих продуктов для управления радиочастотной идентификацией и смежными технологиями. Однако для дальнейшего раскрытия потенциала интернета вещей в военной сфере важно также принимать во внимание новые области исследований, связанные с коммерческим использованием интернета вещей. С точки зрения военного командования и управления, работа гражданских концептов и технологий (например, «умного города») будет сталкиваться со значительными трудностями и сбоями из-за повышенной сложности поля боя и вообще специфичности этой сферы [3, с. 1].

Современная концепция командования, управления, связи и разведки определяется информационными технологиями, которые глубоко внедрены в достижения военного вооружения, что требует высокой эффективности в принятии решений и управлении; более того, такой подход ныне является средством обеспечения превосходства в воздухе, комбинированных воздушно-наземных атак и проецирования военно-морской мощи. В этом подходе технологии и автономность рассматриваются как ключевые факторы, позволяющие выигрывать войны [11. с. 737]. Интернет военных вещей – это сравнительно новая область, использующая технологии интернета вещей в оборонных целях и относимая к взаимосвязанному боевому оборудованию и источникам синхронизированного автоматизированного принятия решений. Из-за сложностей, характерных именно для поля боя, таких, как отсутствие инфраструктуры, разнородность оборудования, сети военного интернета военных вещей значительно отличаются от обычных сетей интернета вещей. В военных сценариях сбор информации о местоположении в режиме реального времени имеет решающее значение для боевой эффективности и зависит от сетевого подключения и обмена информацией в присутствии противника [12, с. 1].

Интернет военных вещей использует многочисленные датчики, развёрнутые в различных областях, для получения полной ситуационной осведомлённости и контроля над различными зонами конфликтов и районами боевых действий. Известно, что передовые государства весьма немало инвестировали в системы и инфраструктуру командования, управления, связи, компьютеров, разведки, наблюдения и рекогносцировки (англ. – «*command, control, communications, computers, intelligence, surveillance, and reconnaissance*» (C4ISR)) вооружённых сил, чтобы собирать, аналитически обрабатывать и передавать данные по назначению. Такие системы обеспечивают необходимую ситуационную осведомлённость. Системы командования и управления позволяют подключённым к ним субъектам оперативно коммуницировать и обмениваться информацией, а система призвана интегрирующе консолидировать всю эту информацию в рамках единой экосистемы. Сети интернета военных вещей способны повысить осведомлённость о ситуации, время реагирования и оценку рисков, на это и рассчитаны. В перспективе для повсеместного развёртывания интернета военных вещей потребуется

операционная система (ОС) для ведения войны [1].

Согласно общему интерпретационному подходу, отражённому в зарубежной научной и специальной литературе, интернет военных вещей предполагает подключение к нему таких военных средств, как наземные транспортные средства, воздушные суда, надводные и подводные суда, в том числе автономные (беспилотные), космические и низкоорбитальные спутники, системы вооружения, а также систем датчиков (способных контролировать условия окружающей среды, отслеживать перемещения, обнаруживать угрозы, измерять производительность или предоставлять информацию о состоянии людей и оборудования), общающихся и обменивающихся данными в режиме реального времени. Такая интеграция позволяет собирать и обрабатывать сверхбольшие массивы и потоки данных из множества распределённых или децентрализованных источников, обеспечивая всестороннее и целостное представление о поле боя, об оперативной обстановке, обеспечивая высокие скорость и эффективность действий бойца и войскового подразделения, командования, обеспечивая им расширенную ситуационную осведомлённость и ситуационную внимательность, необходимые данные о состоянии оборудования, позволяя разрабатывать задачи и делать приближенный к идеальному выбор. Инфраструктура интернета военных вещей опирается на современные сетевые инфраструктуры, включая проводные, беспроводные и гибридные сети, спутниковую связь; при этом применяются защищённые протоколы безопасной связи и протоколы шифрования, системы обнаружения вторжений, комплексные системы кибербезопасности. Эти инфраструктуры обеспечивают необходимую связь для бесперебойного обмена данными и коммуникации между устройствами и системами в различных неблагоприятных и даже экстремальных операционных условиях. Существенную роль в интернете военных вещей играют технологии искусственного интеллекта, в том числе машинного обучения, обеспечивая интеллектуализированную машинно-аналитическую обработку данных (в том числе предиктивную машинную аналитику), машинное распознавание образов (машинное зрение). Они помогают извлекать значимые сведения из огромного количества данных, собранных датчиками, способствуя принятию обоснованных решений в режиме реального времени. При этом экосистема интернета военных вещей должна обладать когнитивными способностями и интегрирующе консолидировать данные от технологических узлов с данными от людей, используя определения местоположения и спутниковый обмен данными, обучаясь на основе предыдущих операций, действуя в настоящем и предиктивно-аналитически оперируя будущими действиями.

Как отмечает Ставрос Апостолопулос, современная сетецентрическая война (англ. – «*network centric warfare*» (NCW)) требует, чтобы военные получали данные на уровне земли с помощью множества датчиков, размещённых на различных платформах. Воздушные сенсорные платформы, спутники наблюдения, наземные станции и солдаты в полевых условиях собирают данные с таких датчиков, как акустическое обнаружение, обнаружение движения, GPS и измерение расстояния. Этот огромный объём данных передаётся в различные военные подразделения и в различные эшелоны военного командования [4, с. 50].

Носимые технологии стремительно внедряются в военном секторе, так как они помогают контролировать физическое состояние бойцов во время миссий, улучшают связь между войсковыми подразделениями и военными постами наблюдения, дают всестороннее знание обстановки. Носимые технологии позволяют командному блоку более точно видеть и отслеживать треки передвижения и текущие позиционирования бойцов, что облегчает контроль за безопасностью бойцов и их скоординированностью во время боевых операций и снижает риск сбоев и ошибок. Ситуационная осведомлённость может быть повышена с помощью технологии визуального интерфейса бойцов с использованием тепловизора, очков ночного видения и технологий дополненной реальности и т. д. Тепловизионная камера может легче обнаруживать и отслеживать движение противника, а очки ночного видения также повышают навык ситуационной осведомлённости в ночное время. Кроме того, технология дополненной реальности используется для быстрого захвата цели путём графического представления ожидаемой ситуации. Комбинация этих технологий позволяет бойцам и командирам лучше понимать окружающую обстановку и быстро решать, что делать дальше. Используя smart-шлемы, smart-очки и носимые видеокамеры, можно улучшить возможности видения и внимания, навыки наблюдения у бойцов. Умный шлем включает в себя «костяные» наушники (с костной проводимостью) для передачи звука, когда боец получает и произносит приказ, вместо традиционных микрофонов и наушников. Умные очки обеспечивают расширенный зрительный обзор и дополнительную информацию с помощью технологий дополненной реальности. Носимая камера может легко собирать визуальную информацию о противнике или своих подразделениях, первично обрабатывая получаемые данные и отсылая их для облачных вычислений. Основываясь на этих носимых датчиках, бойцы могут передавать информацию об индивидуальной ситуации в режиме реального времени, а затем взаимодействовать для выполнения своей миссии (см.: [13, с. 65994–65995]).

V. Авторский концепт интернета военных вещей

Интернет военных вещей – предназначенный для военной сферы (военных действий и контртеррористических операций) сложный мета-системный мультимодульный и мультимодальный комплекс интегрированных посредством специальных протоколов и криптографически-защищённых каналов связи в единую сеть (и соответственно – цифровую экосистему) –

1) средств подключения и рабочих интерфейсов субъектов (бойцов и их подразделений, операторов вооружений, наблюдателей, органов военного управления и др.), **2) функционально совместимых «вещей»** (предметов, периферийных устройств, включая

стационарные, мобильные и носимые устройства, транспортные (в том числе автономные и роботизированные) средства, средства вооружения и боеприпасы, средства индивидуальной защиты, навигации и связи), оснащённых микропроцессорами-контроллерами и / или устройствами мониторинга (датчиками) и средствами (в том числе интерфейсами) подключения к указанной экосистеме, **3) соответствующих цифровых логистических и операционных платформ**, –

обеспечивая в масштабируемых (развёртываемых и свёртываемых) и итеративно-операционабельных модальностях реализацию, комплементарное достраивание функционалов, расширение и усиление возможностей их оперативных совместимости, коммуницирования (обмен данными) и скоординированного применения во взаимодействии с физической средой для выполнения широкого спектра боевых и обеспечительных задач более эффективным и информированным образом.

Аттрактивным центром цифровой экосистемы интернета военных вещей (по сетецентричному принципу) является каждая подключённая к нему боевая единица (боец и командир любого уровня военной иерархии, экипаж боевой техники, штатное войсковое подразделение, тактическая группа),

– чьи встроенные в обмундирование, снаряжение и / или в оружие (а также удалённо дезагрегированно стационарно размещаемые в районе боевых действий и / или размещаемые на дронах и иных подвижных военных средствах) тензодатчики и иные сенсорные, а равно акустические и оптические устройства, а также компактные вычислительные устройства (носимые компьютеры) позволяют этой боевой единице оперативно (непрерывно в режиме реального времени) взаимодействовать с автономными интеллектуальными системами посредством усовершенствованных алгоритмов человеко-машинного взаимодействия,

– чьи средства оперативного приёма данных (smart-микрофоны, мини-дисплеи – дашборды, планшеты, виртуальные ретинальные мониторы (устройства вывода информации, проецирующие изображения непосредственно на сетчатку глаза или на глазную линзу человека; англ. – «*virtual retinal display*», «*retinal scan display*») оперативно поставляют этой боевой единице жизненно важную и важную для выполнения поставленных задач интегрированную информацию о боевой обстановке участка, о состоянии дружественных и вражеских сил, комплементарно достраивая динамически-интегрируемую и корригируемую оперативную картину поля боя и обеспечивая высокую осведомлённость относительно указанного, позволяя видеть оперативную картину поля боя в целом и соответствующие изменения;

– чьи средства вооружения и индивидуальной защиты, боезапасы связаны с сетевыми и встроенными интеллектуализированными ресурсами.

В рамках интернета военных вещей задействуется множество видов и модальностей вычислительных технологий, в их числе:

– **квантовые вычисления** (англ. – «*quantum computing*») – использующие явления квантовой механики и квантовой динамики (квантовая суперпозиция, квантовая запутанность) и оперирующие кубитом как основной единицей информации;

– **пограничные вычисления** (англ. – «*edge computing*») – подразумевающие аналитическую обработку данных как можно ближе к их источнику, а не полагаясь исключительно на централизованную облачную вычислительную инфраструктуру, что позволяет анализировать данные в реальном времени, оперативно проверять их при необходимости и принимать решения на границе сети, сокращая задержки и повышая эффективность работы;

– **облачные вычисления** (англ. – «*cloud computing*») – обеспечивающие масштабируемое и резервируемое хранение данных, необходимые вычислительные мощности и возможности непрерывной в режиме реального времени удалённой машинно-аналитической обработки генерируемых устройствами интернета военных вещей сверхбольших массивов и потоков данных;

– **вычисления в нечёткой логике** (англ. – «*fuzzy logic computing*»).

Концепт интернета военных вещей структурно включает следующие концепты (и соответствующие функционально-технологические модули):

1) концепт цифровой smart-разведки – системы оперативного (непрерывного в режиме реального времени) и интегрированного сбора данных с поля боя (района боевых действий) и с других представляющих интерес территорий, цифрового моделирования поля боя (района боевых действий) и оперативного обеспечения улучшенной ситуационной осведомлённости (англ. – «*enhanced situational awareness*») и ситуационной внимательности, включая тензо-, термо-, электро-магнитные, биометрические и другие датчики, оптические, тепловые (инфракрасные), акустические, радиолокационные системы наблюдения, выявления и фиксации приближения и передвижений противника – его военной техники и личного состава, работы его средств огневого поражения и радиолокации, его пунктов наблюдения и разведки и др., а также носимые бойцами компьютерные устройства, беспилотные летательные аппараты, беспилотные наземные транспортные средства и беспилотные морские транспортные средства, объекты космических и низкоорбитальных спутниковых группировок, интегрируемые в военную сеть для наблюдения, разведки, вскрытия (обнаружения, установления, идентификации) целей, рекогносцировки или для выполнения боевых либо обеспечительных задач (управление огневым воздействием, координация сил и т.д.);

2) концепт цифрового smart-управления в военной сфере:

2.1) системы цифрового обеспечения оперативного командования и сетевой тактической связи и взаимодействия (между личным составом войсковых подразделений, боевой техникой, командными центрами, спутниковой группировкой) в условиях боевых действий, обеспечивая сетецентрические боевые возможности и повышая эффективность и своевременность принятия решений на

поле боя;

2.2) автономные системы цифрового интеллектуализированного боевого управления (на основе синтеза технологий искусственного интеллекта, дополненной реальности, цифровых моделей-двойников и киберметавселенных, робототехники, технологий машинной аналитики), реализующие (автономное вооружение определяется как «системы, которые после активации способны отслеживать, идентифицировать и атаковать цели с применением силы без дальнейшего вмешательства человека» [14, с. 23–24]):

– управление одиночными автономными боевыми средствами (дронами), их группами, эшелонами и роями (см.: [15]);

– управление комплексными огневыми поражениями в отношении сил противника;

– синхронизацию управления личным составом и боевыми техническими средствами;

– применение интеллектуализированного автономного противодействия ракетным ударам противника, с автоматической фиксацией запусков и автоматическим выбором средств поражения ракет противника (лазерное выжигание матрицы головки самонаведения, применение тепловых ловушек и др.);

– управление средствами маскировки, активной постановкой ложных целей и радиопомех;

2.3) концепт «когнитивного поля боя»:

– применение технологий искусственного интеллекта, в том числе алгоритмов машинного обучения, для расширенной предиктивной и прескриптивной аналитической обработки сверхбольших массивов и потоков данных для поддержки принятия решений в режиме реального времени;

– применение технологий цифровых моделей-двойников и киберметавселенных для сценарно-ситуационного моделирования боевых действий и визуализации таких моделирований и их результатов;

– применение технологий дополненной реальности (англ. – «*augmented reality*» (AR)) и виртуальной реальности (англ. – «*virtual reality*» (VR)) для обеспечения необходимого иммерсивного погружения бойца и командира, командного пункта, ситуационного центра военного управления в моделируемые ситуационные сценарии (например, предиктивное моделирование наиболее вероятных сценариев действий противника, предиктивно-аналитическое выявление дезинформации противника), для повышения ситуационной осведомлённости и обеспечения улучшенного ви́дения и понимания оперативной картины поля боя;

2.4) цифровые интеллектуализированные геоинформационные системы, позволяющие получать, аналитически обрабатывать и визуализировать пространственные данные, включая важные геолокационные данные, результаты исследования местностей и планирования маршрутов, обеспечение геоинформационной ситуационной осведомлённости, дистанционного зондирования и глобального позиционирования;

2.5) системы цифрового интеллектуализированного управления военными активами, включая управление логистикой (перемещениями, накоплением, распределением) военных ресурсов, с учётом особенностей местности, погодных условий, действий противника, потребностей своих сил;

3) концепт smart-арсенала (автономные или полуавтономные вооружения и военная техника, подключённые к военным сетям или обладающее встроенными возможностями такого подключения, включая оснащение оружейных магазинов и пакетированных боеприпасов для иного вооружения, либо непосредственно образцов вооружения устройствами отслеживания и индикации расхода боеприпасов и потребностей в них, в том числе для автоматического удалённого формирования логистических запросов на пополнение боеприпасов как для отдельного бойца, так и для войскового подразделения);

4) концепт «smart warrior»:

4.1) системы оперативного (непрерывного в режиме реального времени) и интегрированного мониторинга состояния здоровья и психологического состояния бойца – основанные на встроенных в обмундирование и экипировку бойца трекерах, тензо- и иных датчиках, способных снимать и передавать, непрерывно собирающих и передающих (в том числе с первичной машинно-аналитической обработкой) различные биометрические данные (радужную оболочку глаза, отпечатки пальцев, частоту сердечных сокращений, давление крови, частоту и регулярность дыхания, жесты и мимику, нагрузку в обуви бойцов (см., например: [16]), угрозу или факт растяжения связок голеностопного сустава (см., например: [17]) и мн. др.), результаты машинно-аналитической обработки таковых – о состоянии здоровья, усталости и психологическом состоянии бойца, в том числе для идентификации его на поле боя, в случае его ранения – для формирования рекомендаций по его удалению с поля боя и обеспечения его более точной сортировки в рамках тактической медицины (см.: [18]), для автоматического удалённого формирования логистических запросов на медикаменты и иные средства тактической медицины;

4.2) системы оперативного обеспечения коммуникационных возможностей и ситуационной осведомлённости бойца и командира войскового подразделения, военного командования, – относительно динамически изменяющихся боевых задач, складывающейся боевой обстановки, положения и боевого потенциала противостоящих сил противника, обеспечения улучшенных ви́дения и восприятия бойцом и командиром окружающей обстановки и возможностей боевого взаимодействия с личным составом своего и соседних подразделений, отображение для него помогающей в этом дополненной реальности:

– smart-шлем, встроенные в него или носимые отдельно «костяные» наушники (с костной проводимостью; англ. – «*bone earphones*»);

– носимые, в том числе встроенные, smart-мониторы (дисплеи), smart-часы;

– smart-очки и «умные» глазные линзы;

– носимые видеокамеры;

– сочетание нескольких видов средств

геоинформационного оборудования;

– сочетание нескольких видов коммуникационных устройств – радио- и интернет-связи;

4.3) цифровые smart-системы личного оружия (оружие оснащается интеллектуализированными системами датчиков и исполнительных устройств, обеспечивающих точность, прогнозируемое и настраиваемое запоминание настроек, дают обратную связь об эффективности боевого применения, об истощении боезапаса и времени, через которое потребуется перезарядка и пополнение боезапаса, может быть оснащено средствами биометрии, позволяющими настроить работоспособность оружия исключительно под конкретного бойца);

4.4) цифровые smart-системы обеспечения индивидуальной защиты бойца:

– применение более лёгких и более прочных материалов в броневой защите в целях редуцирования снижения мобильности бойцов, объективно обусловленного её ношением;

– инновационные решения более эффективного рассеяния / поглощения кинетической ударной силы пули или осколка;

– инновационные средства самодиагностики средств индивидуальной защиты и своевременного оповещения бойца и его командования;

– инновационные системы интеллектуализированной трансформации комбинации броневых модулей в средствах индивидуальной защиты, в том числе применение бронежилетов и бронеплит бронежилетов с дифференцированной по толщине твёрдостью;

– применение военных экзоскелетов;

– применение интеллектуальных систем маскировки бойца (включая тестирование качества маскировки);

5) концепт цифровой интеллектуализированной системы оперативной (непрерывной в режиме реального времени) диагностики и прогнозирования состояния вооружений и военной техники (в том числе повреждённости и износа), с удалённым прогнозированием технического обслуживания и ремонта (позволяя проводить проактивное (упреждающее) обслуживание, а не реактивный ремонт, сокращая время простоев и повышая успешность миссий), с формированием логистических запросов на запасные части и принадлежности, ремонтные узлы и агрегаты, на пополнение запасов топлива и смазочных материалов, логистических запросов на техническую эвакуацию с поля боя; управление прогнозируемыми обслуживаниями и ремонтами, заменами и эвакуацией военной техники и вооружений.

Приведённое выше описание структуры не является исчерпывающим, поскольку рассматриваемая сфера постоянно развивается за счёт появления новых технологий, решений, узлов.

VI. Некоторые перспективы развития

Согласно исследовательскому документу организации *GlobalData* 2022 года, весьма затруднительно сколь-нибудь точно оценить сегодня объём рынка интернета военных вещей [1], поскольку многие передовые технические устройства, технологические и компьютерно-программные решения под интернет вещей в военных приложениях, которые исследуются и разрабатываются, тестируются и внедряются, уже применяются, – являются защищёнными режимами военной и государственной тайны. По тем же самым причинам довольно затруднительно определить конкретные государства, добившиеся наибольших успехов в реальном развитии и внедрении интернета военных вещей.

Впрочем, иногда цифры встречаются.

Так, компания Sierra Nevada Corp. (Спаркс, штат Невада, США) получила в декабре 2022 года контракт стоимостью 8 854 602 доллара США с фиксированной оплатой за работу на поставку разработок оперативных замыслов через 5G для военно-морского интернета военных вещей [8] (англ. – «*Navy Internet of Military Things*»).

В аналитическом отчёте организации Market Research Future (MRFR) прогнозировалось, что к 2024 году мировой рынок интернета военных вещей составит 17,7206 млрд долларов США, зафиксировав совокупный годовой темп роста 10,64 % в течение прогнозируемого периода с 2019 по 2024 год. В 2022 году объём рынка военной техники интернета военных вещей оценивался в 11,3 млрд долл. По прогнозам, к 2032 году объём рынка военных технологий интернета военных вещей вырастет до 18,222 млрд, а среднегодовой темп роста (CAGR) составит 6,20 % в течение прогнозного периода (2022–2032) [19].

В любом случае известно, что ведущие военные державы мира рассматривают создание полноценного интернета военных вещей и его развитие как важнейшую часть своей военной стратегии и военно-технической доктрины, обеспечивающую мощные стратегические конкурентные преимущества (англ. – «*competitive advantage*») в военно-технической сфере, в том числе на мировом рынке вооружений, и как важное направление развития военно-промышленного комплекса.

Как пишет Клэр Уитрингтон, базовые формы интернета военных вещей уже существуют и активно применяются, и с развитием технологий вполне вероятно, что их развитие будет продолжаться практически без ограничений. В конечном счёте, вопрос о том, должны ли передовые вооружённые силы продолжать развивать этот потенциал, уже исчерпал себя и ушёл в прошлое, уступив место вопросам о том, как его безопасно и эффективно поддерживать и эксплуатировать [10].

Две существенные особенности применения интернета военных вещей – это выраженно враждебный и жёсткий характер среды поля боя и критические ресурсные проблемы, связанные с энергоснабжением, коммуникациями и централизованными облачными вычислительными архитектурами. Более того, области поля боя, тесно интегрированные с человеческими когнитивными процессами, в будущем потребуют новых или расширения существующих теорий информации, масштабируемых на детерминированные ситуации. Фундаментальные исследования в области технологий, лежащих в основе интернета вещей, таких, как сетевые

технологии, управление информацией и компьютерные архитектуры, будут иметь прямое применение в интернете военных вещей, но враждебный характер поля боя будет представлять собой серьёзную проблему [3, с. 7].

В числе направлений совершенствования систем и комплектующих интернета военных вещей надо выделить следующие:

– развитие систем устойчивой, защищённой и надёжной связи с надёжной аутентификацией;

– выявление и редуцирование уязвимостей кибербезопасности (см.: [20]) (как условий и предпосылок для кибератак, несанкционированного доступа к данным и к управлению подсистемами и устройствами интернета военных вещей, нарушения конфиденциальности данных, перехвата управления военными сетями противником), редуцирование рисков ошибок и сбоев в системах, создание и развитие надёжных методов шифрования, создание безопасных протоколов коммуникаций и обеспечение защиты от кибер-угроз, создание надёжных систем постоянного тестирования безопасности – для обеспечения целостности, конфиденциальности и доступности данных, обмен которыми происходит внутри военных сетей;

– развитие технологий носимых компьютеров и технологий обеспечения гетерогенного доступа в сеть таких военных интеллектуализированных устройств (см.: [13]);

– выявление и редуцирование физических уязвимостей физических устройств интернета военных вещей (от электро-магнитного импульса высокой интенсивности, от ударной волны и осколков, от высоких температур, грязи и пыли, и т.д.);

– повышение энергоэффективности и энергоустойчивости, дальнейшая миниатюризация блоков электропитания устройств интернета военных вещей, развитие энергоэффективных технологий для снижения логистической нагрузки на энергоснабжение, в том числе разработка и интеграция возобновляемых источников энергии, технологий сбора энергии и эффективных систем управления питанием для продления работы устройств интернета военных вещей;

– поиск решений относительно реализации сбора энергии из источников окружающей среды для носимых бойцами устройств интернета военных вещей (в зоне боевых действий умное устройство с малым форм-фактором вообще ограничивает ёмкость аккумулятора и требует частой замены аккумулятора, а зарядка крайне затруднена [13, с. 65997]);

– разработка решений обеспечения защиты и сохранения конфиденциальности местоположения в сетях интернета военных вещей, в том числе с использованием методов, основанных на обмане противника (см.: [12]);

– развитие технологий создания и дальнейшей миниатюризации носимых бойцами устройств интернета военных вещей (сенсорных, мониторинговых, навигационных, телекоммуникационных, целеуказателей и др.) и таких устройств, возимых на военной технике;

– развитие отказоустойчивых и эффективных технологий мощной машинной военной аналитики;

– развитие технологий военных экзоскелетов;

– развитие референтных технологий цифровых моделей-двойников и киберметавселенных (см.: [21]), киберфизических систем, технологий облачных, квантовых и пограничных вычислений;

– развитие технологий производства и применения виртуальных ретинальных мониторов (устройств вывода информации, проецирующих изображение непосредственно на сетчатку глаза или глазную линзу человека);

– развитие технологий производства и применения квантовых тензодатчиков (см.: [22]) и иных инновационных сенсоров;

– редуцирование рисков декогеренции и иных факторов, вносящих шумы в вычисления (в том числе машинно-аналитическую переработку), передачу и отображение сигналов;

– совершенствование точности, надёжности, совместимости и интегрируемости устройств интернета военных вещей;

– поиск решений нравственно-этических и правовых проблем использования автономного оружия, которое потенциально может самостоятельно принимать решения о жизни и смерти без вмешательства оператора-человека (притом что сложное переплетение автономного и запрограммированного поведения в автономных системах вооружений существенно затрудняет понимание проблем, которые они создают [15, с. 3]);

– создание и развитие систем патентно-правовой охраны наиболее существенных для интернета военных вещей решений и узлов, в том числе под видом патентования технологий двойного назначения или гражданских технологий;

– развитие возможностей поддержки интернетом военных вещей функционирования виртуальных учебных сред и обучения на основе симуляций (носимые подключённые устройства интернета военных вещей будут имитировать боевые ситуации в учебно-тренировочных целях);

– развитие нормативно-правового обеспечения интернета военных вещей (по крайней мере, в закрытом режимом государственной тайны сегменте).

VII. Регулирование интернета военных вещей

При наличии ныне в любом развитом крупном государстве множества нормативных правовых актов, регулирующих разработку, патентование, тестирование, применение тех или иных цифровых технологий (например, искусственного интеллекта), по-отдельности лежащих в основе интернета военных вещей, и даже самого интернета вещей (интернета промышленных вещей, интернета медицинских вещей, интернета транспортных вещей и т.д.), отрытого нормативного правового регулирования непосредственно интернета военных вещей нигде не существует.

Это – «серая» или вообще закрытая зона регуляторики. Обоснованно предположить, что непосредственное регулирование интернета военных вещей сводимо к урегулированию секретными актами государственного управления – секретными

нормативными и административно-распорядительными актами. Что-то из указанного может регулироваться на основе регуляторного эксперимента и на основе исключений в праве.

VIII. Заключение

В будущем военная оперативная среда будет представлять собой ландшафт, сочетающий коммерческие / индустриальные информационно-коммуникационные технологии и технологии национальной оборонной науки в многодоменной среде (суша, море, воздух, космос и киберпространство), где организационные границы (объединённая служба, коалиция и т.д.) размыты и интерсекциональны. Многодоменные операции обязательно будут включать технологии сетецентрических войн, а в их числе – и интернет военных вещей [11, с. 737].

Сегодня военные операции стали сложными, многогранными и непредсказуемыми. По мере развития технологических возможностей союзников и противников военное командование вынуждено предвидеть, оценивать и действовать в условиях, которые становятся все более напряжёнными и ограниченными по времени. Некоторые государства начали обращать внимание на потенциальные военные преимущества носимых компьютерных устройств. Автоматизация обороны позволяет современным органам военного управления принимать решения на основе аналитики, производимой в режиме реального времени путём интеграции и обработки информации с широкого спектра носимых и иных мобильных устройств на поле боя [13, с. 66000].

Современная и перспективная военная мощь государства определяется интеллектуальным превосходством (в том числе превосходством в доменной и в ситуационной осведомлённости), достроенным продвинутыми и интегрированными системами оперативного сбора, машинно-аналитической обработки и передачи данных.

И интернет военных вещей – пока наилучшее воплощение этого уже приближающегося будущего.

Благодарности

Настоящим автор выражает благодарность Куприяновскому Василию Павловичу, систематически помогающему интереснейшими материалами и обращающему внимание на интереснейшие аспекты, а также выражает глубокую признательность редакции настоящего журнала.

Библиография

[1] Internet of Military Things – Thematic Research [Интернет военных вещей – тематическое исследование] // <https://www.globaldata.com/store/report/internet-of-military-things-theme-analysis/>. – 10.12.2021.

[2] *Понкин И.В.* Цифра и тенденции развития военных технологий и соответствующей регуляторики: взгляд на зарубежный опыт // International Journal of Open Information Technologies. – 2024. – Vol. 12. – № 2. – С. 75–83.

[3] *Suri N., Tortonesi M., Michaelis J. et al.* Analyzing the Applicability of Internet of Things to the Battlefield Environment [Анализ применимости Интернета вещей в условиях поля боя] // 2016 International Conference on Military Communications and Information Systems (ICMCIS). – Brussels, 2016. <https://ieeexplore.ieee.org/document/7496574>. – 8 p.

[4] *Apostolopoulos S.* Internet of Military Things. Smart Warrior: A thesis submitted for the degree of Master of Science (MSc) in Cybersecurity [Интернет военных вещей. «Умный» воин: Диссертация магистра наук в кибербезопасности] / School of science & technology of the International Hellenic University. – Thessaloniki (Greece), 2022. – xi; 87 p.

[5] Digital Strategy for Defence. Delivering the Digital Backbone and unleashing the power of Defence's data [Цифровая стратегия обороны. Обеспечение цифровой основы и раскрытие потенциала оборонных данных] / UK Ministry of Defence; Directorate of Strategy and Military Digitisation. April 2021 – London, 2021. – 39 p. <https://assets.publishing.service.gov.uk/media/60afae56d3bf7f435f43c7af/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf>.

[6] Defence Artificial Intelligence Strategy 2022. V 1.0, June 2022 [Стратегия оборонного искусственного интеллекта Соединённого Королевства от 2022 г.] / UK Ministry of Defence. – London, 2022. – ii; 68 p.

[7] Summary of NATO's Quantum Technologies Strategy [Резюме Стратегии НАТО в области квантовых технологий] // <https://www.nato.int/cps/en/natohq/official_texts_221777.htm>. – 17.01.2024.

[8] Contracts for Dec. 22, 2022 [Контракты на 22 декабря 2022 года] // <https://www.defense.gov/News/Contracts/Contract/Article/3254039/>.

[9] UK Strategic Commander General Sir Patrick Sanders delivers speech at DSEI 2021 [Командующий стратегическими силами Великобритании генерал Патрик Сандерс выступает с речью на DSEI 2021] // <https://www.gov.uk/government/speeches/uk-strategic-commander-dsei-2021-speech>. – 14.09.2021.

[10] *Withrington C.* The Internet of Military Things [Интернет военных вещей] // <https://cove.army.gov.au/article/internet-military-things>. – 24.08.2023.

[11] *Russell S., Abdelzaher T.* The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making [Интернет вещей поля боя: Следующее поколение принятия решений в области командования, управления, связи и разведки] // MILCOM 2018 – 2018 IEEE Military Communications Conference (MILCOM): Proceedings. – Los Angeles (CA, USA), 2019. – P. 737–742.

[12] *Alkanjr B., Mahgoub I.* Location Privacy-Preserving Scheme in IoBT Networks Using Deception-Based Techniques [Схема сохранения конфиденциальности местоположения в сетях интернета вещей на поле боя с использованием методов, основанных на обмане] //

Sensors. – 2023. – Vol. 23. – № 6. – Article 3142. <https://www.mdpi.com/1424-8220/23/6/3142>. – 19 p.

[13] *Sharma P.K., Park J., Park J.H., Cho K.* Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network [Носимые компьютеры для автоматизации обороны: Возможности и проблемы в сети 5G] // IEEE Access. – 2020. – Vol. 8. – P. 65993–66002.

[14] *Sharkey N.* Staying in the loop: human supervisory control of weapons [Оставаясь в петле: человеческий диспетчерский контроль над вооружениями] // Autonomous Weapons Systems: Law, Ethics, Policy [Автономные системы вооружений: Право, этика, политика] / Edited by Nepal Bhuta, Susanne Beck, Robin Geiβ, Hin-Yan Liu, Claus Kreβ. – Cambridge (United Kingdom): Cambridge University Press, 2017. – x; 410 p. – P. 23–38.

[15] *Weber J.* Autonomous drone swarms and the contested imaginaries of artificial intelligence [Автономные рои дронов и спорные представления об искусственном интеллекте] // <https://link.springer.com/article/10.1057/s42984-023-00076-7>. – 11.01.2024. – 4 p.

[16] *Kong P.W., Iskandar M.N.S., Koh A.H., et al.* Validation of In-Shoe Force Sensors during Loaded Walking in Military Personnel [Валидация датчиков силы в обуви при ходьбе с нагрузкой у военнослужащих] // Sensors. – 2023. – Vol. 23. – № 14. – Article 6465. – 16 p.

[17] *Simpson J.D.; DeBusk H., Hill C., Knight A., Chander H.* The role of military footwear and workload on ground reaction forces during a simulated lateral ankle sprain mechanism [Роль военной обуви и нагрузки на силы реакции на грунт во время моделирования механизма растяжения связок голеностопного сустава] // The Foot. – 2018. – Vol. 34. – P. 53–57.

[18] *Понкин И.В., Шевченко О.А., Понкина А.А.* Регулирование тактической медицины // Военно-медицинское право: Учебник. – Хабаровск: ХГУЭП, 2023. – 200 с. – С. 193–199.

[19] Military loT Market Research Report Information by Component (Hardware, Software and Services), Technology (Wi-Fi, Cellular. RFID and others), Application (Training and Simulation, Health Monitoring, Real-Time Fleet Management, Inventory Management, Equipment Maintenance and others) and Region (North America, Europe, Asia-Pacific, Middle East & Africa and Latin America) - Forecast till 2032. October 2019 // <https://www.marketresearchfuture.com/reports/military-iot-market-7546#>.

[20] *Jang J., Kim K., Yoon S., Lee S., Ahn M., Shin D.* Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage [Анализ влияния на выполнение задач путём измерения влияния на физические боевые операции, связанные с повреждением кибератывов] // IEEE Access. – 2023. – Vol. 11. – P. 45113–45128.

[21] *Понкин И.В.* Военная аналитика. Военное применение искусственного интеллекта и цифры / Консорциум «Аналитика. Право. Цифра». – М.: Буки Веди, 2022. – 106 с. <https://moscou-ecole.ru/ponkin_milit_ai/>.

[22] *Wang X., Lim E.G., Hoettges K., Song P.* A Review of Carbon Nanotubes, Graphene and Nanodiamond Based Strain Sensor in Harsh Environments [Обзор тензодатчиков на основе углеродных нанотрубок, графена и нано-алмаза в жёстких средах] // C. Journal of Carbon Research. – 2023. – № 9 (4). – Article 108. – 37 p.

The Internet of Military Things: Concept, Functional Purpose, Structure, Related Regulatory Developments

Igor Ponkin

***Abstract* – The article is devoted to the study of the role and significance of the concept and technologies of the Internet of Military Things in the competition of military capabilities of the world's leading powers. The article emphasizes that the concept of the Internet of Things as a whole, in principle, originated in the defense community, emerged due to the defense industry's work on sensor networks and low-power computing platforms. The author explains the concept of the Internet of Things, noting the quite expected and logical transition of civilian Internet of Things technologies into military applications. The author briefly shows the importance of the Internet of Military Things given to it in military strategic planning and management documents of a number of foreign countries. The article reviews the explanations of the essence of the Internet of Military Things presented in the scientific literature. The article presents a detailed author's concept of explaining the concept of the Internet of Military Things and its structure. The article discusses the current and potential applications of IoT technologies in the military sphere. The author provides some data on the scale of the market of IoT devices and systems. The author shows two significant features of the application of the Internet of Military Things - 1) the pronounced hostile and harsh nature of the battlefield environment and 2) critical resource issues related to power supply, communications and centralized cloud computing architectures. The paper identifies key future directions for improving the systems and components of the Internet of Military Things. The conclusions are drawn that there is no open normative legal regulation of the Internet of Military Things directly; direct regulation of the Internet of Military Things is reduced to regulation by secret acts of state administration.**

***Keywords* — internet of military things, digitalization of military management, dual-use technologies, artificial intelligence, competition of military advantages, regulatory technologies (RegTech).**

УДК 34:355; 34:007; 34.01; 342; 341; 004.8; 004.9; 681.5
ББК 67:68; 67:30; 67.0; 66.0; 67.4; 67.412; 67.401

Ponkin Igor, Doctor of science (Law), professor of the Institute of Public Administration and Civil Service of the Russian Presidential Academy of National Economy and Public Administration (Moscow, Russia) (IPACS, RANEPA), State professor. (e-mail: ponkin-iv@ranepa.ru).
ORCID: 0000-0003-4438-6649

References

[1] Internet of Military Things – Thematic Research // <https://www.globaldata.com/store/report/internet-of-military-things-theme-analysis/>. – 10.12.2021.

[2] *Ponkin I.V.* Tsifra i tendentsii razvitiia voennykh tekhnologii i sootvetstvuiushchei reguliatoriki: vzgliad na zarubezhnyi opyt [The Digital and the Trends in Military Technology and Related Regulatory Developments: Look at foreign experience] // International Journal of Open Information Technologies. – 2024. – Vol. 12. – № 2. – P. 75–83.

[3] *Suri N., Tortonesi M., Michaelis J. et al.* Analyzing the Applicability of Internet of Things to the Battlefield Environment // 2016 International Conference on Military Communications and Information Systems (ICMCIS). – Brussels, 2016. <https://ieeexplore.ieee.org/document/7496574>. – 8 p.

[4] *Apostolopoulos S.* Internet of Military Things. Smart Warrior: A thesis submitted for the degree of Master of Science (MSc) in Cybersecurity / School of science & technology of the International Hellenic University. – Thessaloniki (Greece), 2022. – xi; 87 p.

[5] Digital Strategy for Defence. Delivering the Digital Backbone and unleashing the power of Defence's data / UK Ministry of Defence; Directorate of Strategy and Military Digitisation. April 2021 – London, 2021. – 39 p. <https://assets.publishing.service.gov.uk/media/60afae56d3bf7f435f43c7af/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf>.

[6] Defence Artificial Intelligence Strategy 2022. V 1.0, June 2022 / UK Ministry of Defence. – London, 2022. – ii; 68 p.

[7] Summary of NATO's Quantum Technologies Strategy // <https://www.nato.int/cps/en/natohq/official_texts_221777.htm>. – 17.01.2024.

[8] Contracts for Dec. 22, 2022 // <https://www.defense.gov/News/Contracts/Contract/Article/3254039/>.

[9] UK Strategic Commander General Sir Patrick Sanders delivers speech at DSEI 2021 // <https://www.gov.uk/government/speeches/uk-strategic-commander-dsei-2021-speech>. – 14.09.2021.

[10] *Withrington C.* The Internet of Military Things // <https://cove.army.gov.au/article/internet-military-things>. – 24.08.2023.

[11] *Russell S., Abdelzaher T.* The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making // MILCOM 2018 – 2018 IEEE Military Communications Conference (MILCOM): Proceedings. – Los Angeles (CA, USA), 2019. – P. 737–742.

[12] *Alkanjr B., Mahgoub I.* Location Privacy-Preserving Scheme in IoBT Networks Using Deception-Based Techniques // Sensors. – 2023. – Vol. 23. – № 6. –

Article 3142. <https://www.mdpi.com/1424-8220/23/6/3142>. – 19 p.

[13] *Sharma P.K., Park J., Park J.H., Cho K.* Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network // IEEE Access. – 2020. – Vol. 8. – P. 65993–66002.

[14] *Sharkey N.* Staying in the loop: human supervisory control of weapons [Оставаясь в петле: человеческий диспетчерский контроль над вооружениями] // Autonomous Weapons Systems: Law, Ethics, Policy / Edited by Nepal Bhuta, Susanne Beck, Robin Geiβ, Hin-Yan Liu, Claus Kreβ. – Cambridge (United Kingdom): Cambridge University Press, 2017. – x; 410 p. – P. 23–38.

[15] *Weber J.* Autonomous drone swarms and the contested imaginaries of artificial intelligence // <https://link.springer.com/article/10.1057/s42984-023-00076-7>. – 11.01.2024. – 4 p.

[16] *Kong P.W., Iskandar M.N.S., Koh A.H., et al.* Validation of In-Shoe Force Sensors during Loaded Walking in Military Personnel // Sensors. – 2023. – Vol. 23. – № 14. – Article 6465. – 16 p.

[17] *Simpson J.D.; DeBusk H., Hill C., Knight A., Chander H.* The role of military footwear and workload on ground reaction forces during a simulated lateral ankle sprain mechanism // The Foot. – 2018. – Vol. 34. – P. 53–57.

[18] *Ponkin I.V., Shevchenko O.A., Ponkina A.A.* Regulirovanie takticheskoi meditsiny [Regulation of tactical medicine] // Military Medical Law: Textbook. – Khabarovsk, 2023. – 200 p. – P. 193–199.

[19] Military loT Market Research Report Information by Component (Hardware, Software and Services), Technology (Wi-Fi, Cellular. RFID and others), Application (Training and Simulation, Health Monitoring, Real-Time Fleet Management, Inventory Management, Equipment Maintenance and others) and Region (North America, Europe, Asia-Pacific, Middle East & Africa and Latin America) - Forecast till 2032. October 2019 // <https://www.marketresearchfuture.com/reports/military-iot-market-7546#>.

[20] *Jang J., Kim K., Yoon S., Lee S., Ahn M., Shin D.* Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage // IEEE Access. – 2023. – Vol. 11. – P. 45113–45128.

[21] *Ponkin I.V.* Voennaia analitika. Voennoe primenenie iskusstvennogo intellekta i tsifry [Military analytics: Military applications of Artificial Intelligence and digital technologies]. – Moscow: Buki Vedi, 2022. – 106 p. <https://moscou-ecole.ru/ponkin_milit_ai/>.

[22] *Wang X., Lim E.G., Hoettges K., Song P.* A Review of Carbon Nanotubes, Graphene and Nanodiamond Based Strain Sensor in Harsh Environments // C. Journal of Carbon Research. – 2023. – № 9 (4). – Article 108. – 37 p.