Журнал "Мировые цивилизации" / Scientific journal "World civilizations" https://wcj.world

2020, №3–4, Том 5 / 2020, No 3–4, Vol 5 https://wcj.world/issue-3-4-2020.html

URL статьи: https://wcj.world/PDF/02ECMZ320.pdf

Ссылка для цитирования этой статьи:
Рольф Клауберг Киберфизические системы и искусственный интеллект: шансы и угрозы для современной экономики // Мировые цивилизации, 2020 №3–4, https://wcj.world/PDF/02ECMZ320.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Rolf Clauberg (2020). Cyber-physical systems and artificial intelligence: chances and threats to modern economies. *World civilizations*, [online] 3–4 (5). Available at: https://wcj.world/PDF/02ECMZ320.pdf (in Russian)

УДК 33

Рольф Клауберг
ФГАОУ ВО «Российский университет дружбы народов», Москва, Россия
Доцент кафедра «Менеджмента» «Экономического» факультета
Компания «InterKulturForum», Цюрих, Швейцария
Генеральный директор
Кандидат естественный наук: направление – физика
E-mail: r.clauberg@hispeed.ch; klauberg-r@rudn.ru
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=1067538
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=6603566417

Киберфизические системы и искусственный интеллект: шансы и угрозы для современной экономики

Аннотация. В данной статье дается анализ потенциальных возможностей и угроз для современных цивилизаций и экономики, обусловленных киберфизическими системами и искусственным интеллектом. На основе исследовательских работ, описывающий эволюцию кибер-физических систем и искусственного интеллекта, анализируется для выявления глубинных сил, движущих этими эволюциями, и потенциальных возможностей, создаваемых этими новыми технологиями, а также наиболее серьезных угроз, исходящих от них. Особое внимание уделяется слиянию операционных и информационных технологий, а также соответствующих киберфизических систем в критической инфраструктуре, на промышленных предприятиях и в беспилотных летательных аппаратах. Для киберфизических систем в критической инфраструктуре и промышленных предприятиях мы находим шансы, определяющие эволюцию, главным образом в повышении производительности и повышении эффективности и простоты использования на существующих рынках. Для беспилотных летательных аппаратов соответствующие шансы имеют в основном новые области применения, на рынках, доступных ранее только с высоким риском для жизни и здоровья человека. Для угроз делается попытка оценить размер угроз от предыдущих событий и потенциал реализации этих угроз из того, что необходимо для реализации и что легко доступно с точки зрения аппаратного обеспечения, программного обеспечения и технических знаний. Угрозы для обеих областей заключаются, главным образом, в кибертерроризме и кибервойне.

Ключевые слова: искусственный интеллект; кибербезопасность; кибертерроризм; кибер-физические системы; цифровизация; беспилотные летательные аппараты

Введение

Сегодняшняя цифровизация, в основном, началась после «*кризисов доткомов 2000 г.*» (англ. – dot.com crisis 2000), следствием чего стали – развитие электронной коммерции, электронных закупок, цифровых рынков, цифровых цепочек создания стоимости, электронных услуг, бизнес-моделей и технологий для цифрового бизнеса [1]. Она сопровождалась глобализацией торговли [2] и соответственно интегрированными цепочками создания стоимости. В корне изменилась деятельность многих компаний, которую Сэмюэл Дж. Палмисано (председатель, президент и генеральный директор корпорации IBM) охарактеризовал в 2006 году как *«глобально интегрированным предприятием»* (англ. – globally integrated enterprise)[1]. Такого рода предприятие имело конкретные корпоративные функции, которые были сосредоточены в любой точке земного шара и имели оптимальные условия для развития этой компании.

В индустриальной сфере эта эволюция привела к появлению так называемого *«Промышленного интернета вещей»* (ПИВ), (англ. – Industrial Internet of Things, IIoT) [3]. Тем самым, стал развиваться процесс внедрения в интернет *«автоматизированных систем управления технологическими процессами»* (АСУ ТП, англ. – ICS) и *«систем диспетчерского контроля, управления и сбора данных»* (Supervisory Control And Data Acquisition, SCADA), в результате чего представители бизнеса получили прямой доступ к данным о промышленных процессах. Это соединение между операционной и информационной технологиями создает киберфизические системы, позволяет осуществлять глобальную интеграцию и автоматизацию цепочек поставок. Это также важный аспект в создании и развитии цифрового предприятия – "Промышленность 4.0" и "умные заводы" [4], которые оба нацелены на высокоавтоматизированные заводы, в которых можно модифицировать продукт или даже перейти на другой продукт, просто изменив входные данные, подаваемые в компьютерную систему управления завода. Это возможно при почти полной автоматизации, когда все производственные процессы контролируются датчиками, которые измеряют все виды информации о состоянии производственных процессов. Эта информация затем используется для автоматического управления производственными процессами.

Генерация огромного количества сенсорных данных в рамках «Промышленного интернета вещей» требует автоматической обработки информации. В настоящее время это поддерживается искусственным интеллектом (ИИ, англ. *artificial intelligence, AI*). В системах ICS/SCADA это было, в основном, ограничено «алгоритмическим искусственным интеллектом». Однако, «нейросетевой искусственный интеллект» уже встречается для распознавания обнаружения вторжений в информационную технологию и киберфизические системы [5].

Второй областью, где киберфизические системы работают совместно с искусственным интеллектом, являются автономные или полуавтономные беспилотные летательные аппараты (БПЛА, англ. – *unmanned aerial vehicle, UAV*) [6]. БПЛА широко используются в промышленной инспекции, а также в картографировании и геодезии.

Киберфизические системы и искусственный интеллект – то две новые технологии, которые сильно влияют на цифровизацию нашего современного мира.

Далее в статье будут описаны методы, представлены возможности и угрозы киберфизических систем и искусственного интеллекта и, наконец, будут сделаны выводы.

[1] The Globally Integrated Enterprise [Электронный ресурс] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/globalbiz/transform/ (дата обращения: 03.12.2018).

Методы

Основным методом изучения является анализ цитируемых научно-исследовательских ресурсов с тем, чтобы выявить главные движущие силы такой специфической тенденции, как переход от разрозненных систем операционной техники и информационных технологий к единой системе с киберфизическими единицами или взрывное использование искусственного интеллекта. Затем будет дан анализ новых технологий, чтобы найти их наиболее перспективные приложения, а также серьезные угрозы и вероятность реализации этих угроз.

Обсуждение

Если рассматривать киберфизические системы в рамках критической инфраструктуры или промышленных предприятий, то все преимущества соединения оперативной технологии с интернетом связаны с повышением производительности за счет более легкого доступа к оперативным или производственным данным. С одной стороны, данные из операционной технологии могут быть доступны бизнесменам, а высоко агрегированные и обработанные данные обеспечивают понимание операционных и производственных процессов. Это позволяет оптимизировать и адаптировать эти процессы. С другой стороны, обновление программного обеспечения для операционных технологических систем может быть проще и быстрее реализовано [3; 4].

В случае рассмотрения угрозы критической инфраструктуры и промышленных предприятиях, то они, в основном, связаны с кибертерроризмом и кибервойной. Мы должны учитывать ущерб, который может быть причинен соответствующими атаками, а также сложность или легкость их выполнения. Критическая инфраструктура включает в себя энергетические, водные и транспортные сети (воздушные, автомобильные, речные). Из опыта Второй мировой войны становится ясно, что атаки на подобные объекты инфраструктуры могут нанести решающий ущерб экономике, а также здоровью и жизни людей. Вторым примером разрушительного ущерба, причиненного промышленной аварией, является Бхопальская катастрофа 1984 года в Индии [7]. Это авария, вызванная малоэффективными или отсутствующими системами безопасности, стоила жизни тысячам людей[2]. Вопрос заключается в том, может ли подобная авария сегодня быть вызвана кибератаками через интернет. Ответ на этот вопрос зависит от двух факторов. Прежде всего, от того, существуют ли сегодня такого рода вредоносные программы – компьютерных вирусов или «червей», способные манипулировать эксплуатационными параметрами киберфизических систем. Во-вторых, существует ли эффективная система компьютерной безопасности, способная гарантировать защиту от кибератак.

Наиболее наглядным примером комплексной и специфической компьютерной атаки является вредоносная компьютерная программа «червь Stuxnet» [8]. После того, как программа проникала в определенный компьютер, она начала искать определенные специальные программируемые логические контроллеры. Если таковые были подключены к этому компьютеру и выполнялись другие условия, программа становилась активной и начинала свою деструктивную деятельность. Она изменяла рабочие параметры контролируемых промышленных систем таким образом, чтобы система уничтожалась, не посылая тревожных сигналов. Этот пример ясно показывает, что возможны целенаправленные атаки на определенные киберфизические системы. Программа "червь Stuxnet" достигала свои целей

[2] Encyclopedia Britannica. [Электронный ресурс]. URL: https://www.britannica.com/event/Bhopal-disaster (дата обращения: 19.03.2020).

через обновления программного обеспечения со встроенными USB-накопителями. В настоящее время эти вредоносные программы доступны непосредственно через интернет.

Следует отметить, что операционно-технологические системы несколько лучше защищены, чем «чистые» информационно-технологические системы. Они используют, например, так называемые демилитаризованные зоны с сетевыми двойными экранами (брандмауэрами, англ. firewall). Кроме того, были проведены оценки аспектов безопасности для киберфизических систем [9–11], касающихся конкретных аспектов таких систем. Однако общая степень защищенности обоих систем, операционно-технологических и информационно-технологических, до сих пор не является убедительной. Институт Понемона, занимающийся вопросами сохранения данных и новых компьютерных технологий в мире, подготовил при спонсорской поддержке американского концерна IBM доклад под названием «2017 Cost of Data Breach Study» [3]. Этот документ представляет собой научное исследование по вопросам компьютерной безопасности в 419 компаниях в 13 странах и 2 регионах мира. Среди этих стран – США, Великобритания, Германия, Австралия, Франция, Бразилия, Япония, Италия, Индия, Канада и Южная Африка. В докладе речь идет о двух регионах – Ближний Восток и страны АСЕАН (Ассоциация государств Юго-Восточной Азии). В этом документе (рисунок 22 на стр. 27) отмечается, что среднее время для выявления нарушения данных, вызванного злонамеренной или преступной атакой, составляет примерно 214 дней. После выявления нарушения требуется еще примерно 77 дней для поддержания нарушения данных. В итоге, делается вывод о том, что это довольно значительное время для компьютерного вируса и червя, чтобы проанализировать всю систему и выполнить соответствующую атаку.

В отношении беспилотных летательных аппаратов (БПЛА) следует отметить, что их использование, в основном, связано с контролем, ремонтом и спасательными работами. То есть там, где человеческая деятельность трудна или опасна. Они используются в ситуациях, когда требования к быстрому времени отклика делают дистанционное управление невозможным или, по крайней мере, непрактичным [6] . Таким образом, в отличие от киберфизических систем в критических инфраструктурах или промышленных предприятиях, БПЛА являются важным элементом современной жизни, а не просто вопросом удобства или повышения эффективности. Многие работы, которые сейчас выполняются автономными беспилотными летательными аппаратами ранее были невозможны. Современные приложения, в основном, используют оптическую систему для навигации БПЛА и оптического обнаружения определенных объектов. В обоих случаях они используют информационно-технологические системы, основанные на алгоритмах [12; 13] или нейронные сети [14; 15].

Как и в случае с киберфизическими системами, БПЛА представляют серьезную угрозу в кибервойне и кибертерроризме. Автономные БПЛА способны выслеживать конкретные цели, распознавать конкретные объекты и затем предпринимать заданные программой действия. Распознавание объектов обычно выполняется с использованием нейронных сетей, что до сих пор является несовершенным. Возникает проблема, когда в конкретных ситуациях происходит ошибочная идентификация объекта с высокой степенью точности. [16]. Кроме того, возникают ошибки, если материалы для нейронной сети плохо подготовлены и проанализированы. Военное руководство различных стран неохотно использует автономные системы БПЛА во время военных действий для уничтожения целей. Обычно они используют их в сочетании с дистанционным управлением человеком, что позволяет человеку решать, следует ли наносить удар после автономного обнаружения цели. Однако террористические группы не всегда ориентированы на точное попадание в цель. Итак, можно сказать, что БПЛА – системы могут быть использованы для уничтожения конкретных целей. Вопрос состоит в том, насколько легко

[3] 2017 Cost of Data Breach Study [Электронный ресурс]. URL: https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states?s=2017+Cost+of+Data+Breach+Study (дата обращения: 19.03.2020).

для террористической группы построить такой автономный беспилотник. Судя по публикациям, которые приводились выше, существуют небольшие группы в университетах разных стран, которые успешно построили свои собственные автономные беспилотники. Важным моментом является то, что все аппаратные компоненты для построения БПЛА-системы можно свободно купить на рынке и по довольно низким ценам. В частности, помимо графических процессоров, которые были первым видом ускорителей для операций с нейронными сетями искусственного интеллекта, Google разработала специальные ТП (тензорные процессоры[4]), которые предлагают соответствующие возможности при гораздо меньшем энергопотреблении и меньших габаритах. Кроме того, некоторые организации предлагают соответствующее программное обеспечение и учебные материалы даже бесплатно[5]. Таким образом, можно сделать вывод, что сегодня даже небольшие группы людей способны создавать автономные БПЛА-системы и по низкой стоимости. Достаточно того, чтобы в состав такой группы входили специалисты, обладающих необходимыми навыками для построения небольших аппаратных систем из компонентов, имелся открытый доступ к приобретению необходимых деталей (к примеру, на рынке) и адаптации свободно доступных программных пакетов к конкретным целям.

Одной из самых обсуждаемых тем в мировом сообществе является искусственный интеллект и его влияние на мировой рынок труда. Прежде всего, изучается вопрос о том, какие профессии исчезнут в будущем и какие новые специальности появятся. Этой теме был посвящен доклад Национальной академии наук США [17], в котором рассматривались различные точки зрения, в частности, предвидения, опасения, возможные сценарии развития (оптимистические и пессимистические), а также реальные перспективы. Результатом этого доклада стал вывод о том, что исследователи и политики в разных странах в настоящее время не готовы спрогнозировать изменения на мировом рынке труда. Никто сейчас не может дать точную оценку и предсказать ситуацию с применением искусственного интеллекта в самых разных отраслях. Единственный реалистичный вывод заключается в том, что искусственный интеллект будет оказывать значительное влияние на рабочее пространство человека. В частности, люди должны научиться использовать искусственный интеллект в определенной области. Конечно, это приведет к определенному переформатированию рынка труда – одни рабочие места будут уничтожены, а другие, наоборот, появятся. Новые профессии требуют приобретения новых навыков и профессиональных знаний. В отличие от промышленной автоматизации, искусственный интеллект может также уничтожить рабочие места для высокообразованных людей. Так, сегодня юридические фирмы в разных странах, применяющие "прецедентное право" (например, в США и Великобритании), используют молодых юристов для анализа судебных решений и использования полученных результатов в качестве аргументов в текущих делах. Кроме того, медицина использует высокообразованных людей для анализа результатов компьютерной томографии с целью выявления тех или иных заболеваний. В обоих случаях анализ, проведенный искусственным интеллектом, может дать лучшие результаты, чем человеческая деятельность. И завтра это может стать реальностью.

[4] Edge Tensor Processing Units – [Электронный ресурс]. URL: https://aiyprojects.withgoogle.com/edge-tpu/ и небольшие локальные платформы искусственного интеллекта – https://coral.ai/ (дата обращения: 19.03.2020).

[5] TensorFlow – это сквозная платформа с открытым исходным кодом для машинного обучения. Robot Operating System (ROS) – это гибкая основа для написания программного обеспечения робота. – [Электронный ресурс]. URL: https://www.tensorflow.org/, https://www.ros.org/ (дата обращения: 19.03.2020).

Выводы

Движущей силой в интеграции двух систем – операционной технологии и информационной технологии – в инфраструктуре и промышленных системах явно является создание экономических преимуществ за счет повышения эффективности и производительности за счет облегчения обмена данными между двумя этими системами. Вместе с «умными фабриками» они позволяют осуществлять высокоавтоматизированные операции в глобальных цепочках поставок и создания стоимости.

Для автономных и полуавтономных БПЛА движущей силой является возможность выполнять различные мероприятия (дистанционный осмотр, геодезия, спасательные операции в опасных районах), которые наиболее опасны для людей. Раньше эти рынки были недоступны без серьезного воздействия на людей этих опасностей. Использование искусственного интеллекта в автономных БПЛА всегда является необходимостью. Основные угрозы для обеих областей базируются на кибертерроризме и кибервойне против людей и экономики. Для автономных или полуавтономных БПЛА это означает злоупотребление этими системами для выполнения атак на определенные цели.

Для киберфизических систем это означает атаки компьютерных вирусов или червей на эти системы, приводящие к потенциально катастрофическому ущербу для общества и экономики. Для этих областей потенциальные угрозы являются серьезными, и возможность выполнения этих угроз вполне реальна. В области критической инфраструктуры и промышленных предприятий значительные меры по повышению безопасности системы могут снизить уровень угроз. В зоне действия автономных БПЛА наблюдение за воздушным пространством вплоть до объектов размером с беспилотники, способных нести бомбы или опасное оружие, может быть единственным решением для снижения этих угроз.

С учетом влияния искусственного интеллекта на мировой рынок труда, в качестве лучшей мерой для защиты рабочих мест следует на рассматривать непрерывное профессиональное образование и более широкое базовое образование, что позволит быстрее адаптироваться к новым рабочим местам в меняющемся мировом рынке труда.

Перевод с английского сделала Н.И. Маслакова-Клауберг

ЛИТЕРАТУРА

1. Fingar P., Aronica R. Death of “e” and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century. Tampa, Fl, USA: Meghan-Kiffer Press, 2001. 360 p.
2. Friedman T.L.T. The world is flat: A brief history of the twenty-first century // New York: Farrar, Straus and Giroux. New York, NY, USA: Farrar, Straus and Giroux, 2007. 660 p.
3. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems // Industrial Internet of Things / ed. Jeschke S., Brecher C., Song H.R.D. Cham: Springer International Publishing Switzerland, 2017. P. 3–19.
4. Almada-Lobo F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) // J. Innov. Manag. 2016. Vol. 3, № 4. P. 16–21.

5. Kathareios G. et al. Catch it if you can: Real-time network anomaly detection with low false alarm rates // Proceedings – 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017. Institute of Electrical and Electronics Engineers Inc. (IEEE), 2017. P. 924–929.
6. Lu Y. et al. A survey on vision-based UAV navigation // Geo-Spatial Inf. Sci. Taylor & Francis, 2018. Vol. 21, № 1. P. 21–32.
7. Yang M., Khan F., Amyotte P. Operational risk assessment: A case of the Bhopal disaster // Process Saf. Environ. Prot. 2015. Vol. 97. P. 70–79.
8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security // IECON Proceedings (Industrial Electronics Conference). 2011. P. 4490–4494.
9. Lu T. et al. Towards a framework for assuring cyber physical system security // Int. J. Secur. its Appl. 2015. Vol. 9, № 3. P. 25–40.
10. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA // Int. J. Cyber Warf. Terror. 2016. Vol. 6, № 3. P. 1–16.
11. Wu W., Kang R., Li Z. Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities // IEEE International Conference on Industrial Engineering and Engineering Management. 2016. P. 1618–1622.
12. Opromolla R., Fasano G., Accardo D. A vision-based approach to uav detection and tracking in cooperative applications // Sensors (Switzerland). 2018. Vol. 18, № 10.
13. Suleiman A. et al. Navion: A 2-mW Fully Integrated Real-Time Visual-Inertial Odometry Accelerator for Autonomous Navigation of Nano Drones // IEEE J. Solid-State Circuits. 2019. Vol. 54, № 4. P. 1106–1119.
14. Palossi D. et al. A 64-mW DNN-Based Visual Navigation Engine for Autonomous Nano-Drones // IEEE Internet Things J. Institute of Electrical and Electronics Engineers Inc., 2019. Vol. 6, № 5. P. 8357–8371.
15. Wyder P.M. et al. Autonomous drone hunter operating by deep learning and all-onboard computations in GPS-denied environments // PLoS One. 2019. Vol. 14, № 11. P. 1–18.
16. Hendrycks D. et al. Natural Adversarial Examples [Electronic resource]. 2019. URL: https://arxiv.org/pdf/1907.07174.pdf.
17. Frank M.R. et al. Toward understanding the impact of artificial intelligence on labor // Proceedings of the National Academy of Sciences of the United States of America. 2019. P. 9.

Rolf Clauberg
Peoples' friendship university of Russia, Moscow, Russia
«InterKulturForum» GmbH, Zürich, Schweiz
E-mail: r.clauberg@hispeed.ch; klauberg-r@rudn.ru
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=1067538
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=6603566417

Cyber-physical systems and artificial intelligence: chances and threats to modern economies

Abstract. This article analyzes the potential chances and threats to modern civilizations and economies caused by cyber-physical systems and artificial intelligence. Literature describing the evolution of cyber-physical systems and artificial intelligence is analyzed for discerning the underlying forces driving these evolutions, the potential chances brought by these new technologies as well as the most serious threats stemming from these technologies. Special emphasize is given to the merge of operational technology and information technology and corresponding cyber-physical systems in critical infrastructure, industrial plants, and unmanned aerial vehicles. For cyber-physical systems in critical infrastructure and industrial plants we find the chances driving the evolution mainly in enhancements of productivity and improvements of efficiency and ease of use within their existing markets. For unmanned aerial vehicles the corresponding chances are mainly new applications, in markets accessible before only with high risk for human life and health. For the threats we try to estimate the size of threats from previous events and the potential to realize these threats from what is needed for the realization and what is easily available in terms of hardware, software, and technical knowledge. The threats for both areas are mainly in cyber-terrorism and cyber-warfare.

Keywords: artificial intelligence; cyber-security; cyber-terrorism; cyber-physical systems; digitalization; unmanned aerial vehicles

REFERENCES

1. Fingar P., Aronica R. Death of "e" and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century. Tampa, Fl, USA: Meghan-Kiffer Press, 2001. 360 p.
2. Friedman T.L.T. The world is flat: A brief history of the twenty-first century // New York: Farrar, Straus and Giroux. New York, NY, USA: Farrar, Straus and Giroux, 2007. 660 p.
3. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems // Industrial Internet of Things / ed. Jeschke S., Brecher C., Song H.R.D. Cham: Springer International Publishing Switzerland, 2017. P. 3–19.
4. Almada-Lobo F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) // J. Innov. Manag. 2016. Vol. 3, № 4. P. 16–21.
5. Kathareios G. et al. Catch it if you can: Real-time network anomaly detection with low false alarm rates // Proceedings – 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017. Institute of Electrical and Electronics Engineers Inc. (IEEE), 2017. P. 924–929.
6. Lu Y. et al. A survey on vision-based UAV navigation // Geo-Spatial Inf. Sci. Taylor & Francis, 2018. Vol. 21, № 1. P. 21–32.

7. Yang M., Khan F., Amyotte P. Operational risk assessment: A case of the Bhopal disaster // Process Saf. Environ. Prot. 2015. Vol. 97. P. 70–79.
8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security // IECON Proceedings (Industrial Electronics Conference). 2011. P. 4490–4494.
9. Lu T. et al. Towards a framework for assuring cyber physical system security // Int. J. Secur. its Appl. 2015. Vol. 9, № 3. P. 25–40.
10. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA // Int. J. Cyber Warf. Terror. 2016. Vol. 6, № 3. P. 1–16.
11. Wu W., Kang R., Li Z. Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities // IEEE International Conference on Industrial Engineering and Engineering Management. 2016. P. 1618–1622.
12. Opromolla R., Fasano G., Accardo D. A vision-based approach to uav detection and tracking in cooperative applications // Sensors (Switzerland). 2018. Vol. 18, № 10.
13. Suleiman A. et al. Navion: A 2-mW Fully Integrated Real-Time Visual-Inertial Odometry Accelerator for Autonomous Navigation of Nano Drones // IEEE J. Solid-State Circuits. 2019. Vol. 54, № 4. P. 1106–1119.
14. Palossi D. et al. A 64-mW DNN-Based Visual Navigation Engine for Autonomous Nano-Drones // IEEE Internet Things J. Institute of Electrical and Electronics Engineers Inc., 2019. Vol. 6, № 5. P. 8357–8371.
15. Wyder P.M. et al. Autonomous drone hunter operating by deep learning and all-onboard computations in GPS-denied environments // PLoS One. 2019. Vol. 14, № 11. P. 1–18.
16. Hendrycks D. et al. Natural Adversarial Examples [Electronic resource]. 2019. URL: https://arxiv.org/pdf/1907.07174.pdf.
17. Frank M.R. et al. Toward understanding the impact of artificial intelligence on labor // Proceedings of the National Academy of Sciences of the United States of America. 2019. P. 9.