Человек: преступление и наказание. 2022. Т. 30(1–4), № 3. ISSN 1999-9917 (print). ISSN 2687-1238 (online)
Man: crime and punishment, 2022, vol. 30(1–4), iss. 3, ISSN 1999-9917 (print), ISSN 2687-1238 (online)

Научная статья
УДК 007
Doi: 10.33463/2687-1238.2022.30(1-4).3.326-335

МЕТОДЫ И ИНСТРУМЕНТЫ ВЕДЕНИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ: НОВЫЕ УГРОЗЫ ПОДРЫВА СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ И ПОЛИТИЧЕСКОЙ СТАБИЛЬНОСТИ ГОСУДАРСТВА

Михаил Николаевич Козин[1], Алексей Владимирович Родионов[2]
[1] НИИ ФСИН России, г. Москва, Россия, kozin-volsk@mail.ru, http://orcid.org/0000-0002-2107-1882
[2] Академия ФСИН России, г. Рязань, Россия, avrpost@bk.ru, http://orcid.org/0000-0002-9311-4896

Аннотация. В статье исследуются проблемы информационной войны с позиции разрешения комплекса экономических, морально-политических, технологических факторов, а также технологических возможностей массовой сетевой коммуникации. Целью исследования является систематизация методов и инструментов ведения информационной войны, обеспечивающей повышение эффективности мобилизации сил и ресурсов Российской Федерации в отношении осуществления информационной защиты индивидуального и общественного сознания российского общества. В качестве объекта исследования выступают организационно-экономические процессы, складывающиеся при обосновании и реализации активных мероприятий по противодействию психологическим и информационно-техническим операциям. Исследование основывается на научных трудах отечественных и зарубежных авторов в области теории национальной и информационной безопасности, методах анализа, синтеза и классификации. Отмечается, что относительно небольшие силы и средства при незначительных финансовых затратах позволяют вывести из строя военную и государственную информационную инфраструктуру, достичь и удержать информационное превосходство и защиту собственной информации и информационных систем. В процессе проведенного анализа показана необходимость мобилизации ресурсов и всего российского общества, построения высокоэффективной и малобюджетной интегрированной системы противодействия психологическим и информационно-техническим операциям. Такой подход позволяет перевести информационную войну из разряда скрытых угроз в явную и обосновать применение необходимых сил, средств, а также мер корректирующего и предупреждающего воздействия в рамках единой стратегии обеспечения национальной безопасности Российской Федерации.

Ключевые слова: информационная война, метод, инструмент, угроза, стабильность, государство, социально-экономическая и политическая стабильность

Для цитирования
Козин М. Н., Родионов А. В. Методы и инструменты ведения информационной войны: новые угрозы подрыва социально-экономической и политической стабильности государства // Человек: преступление и наказание. 2022. Т. 30(1–4), № 3. С. 326–335. DOI : 10.33463/2687-1238.2022.30(1-4).3.326-335.

Original article

METHODS AND TOOLS OF INFORMATION WARFARE: NEW THREATS TO UNDERMINE THE SOCIO-ECONOMIC AND POLITICAL STABILITY OF THE STATE

Mikhail Nikolaevich Kozin[1], Aleksey Vladimirovich Rodionov[2]
[1] Research Institute of the FPS of Russia, Moscow, Russia, kozin-volsk@mail.ru, http://orcid.org/0000-0002-2107-1882
[2] Academy of the FPS of Russia, Ryazan, Russia, avrpost@bk.ru, http://orcid.org/0000-0002-9311-4896

Abstract. The article is devoted to the problems of information warfare from the perspective of resolving a complex of economic, moral, political, technological factors, as well as technological capabilities of mass network communication. The purpose of the study is to systematize methods and tools of information warfare, ensuring an increase in the effectiveness of the mobilization of forces and resources of the Russian Federation in relation to the implementation of information protection of individual and public consciousness of the Russian society. The object of the study is the organizational and economic processes that develop during the justification and implementation of active measures to counter psychological and information technology operations. The research is based on the scientific works of domestic and foreign authors in the field of national and information security theory, methods of analysis, synthesis and classification. It is noted that relatively small forces and means at insignificant financial costs make it possible to disable the military and state information infrastructure, achieve and maintain information superiority and protect their own information and information systems. The analysis shows the need to mobilize resources and the entire Russian society, to build a highly effective and low-budget integrated system to counter psychological and information technology operations. Such a new approach makes it possible to transfer the information war from the category of hidden threats to an explicit one and justify the use of the necessary forces, means, as well as corrective and preventive measures within the framework of a unified strategy for ensuring the national security of the Russian Federation.

Keywords: information warfare, method, tool, threat, stability, states, socio-economic and political stability

For citation
Kozin, M. N. & Rodionov, A. V. 2022, 'Methods and tools of information warfare: new threats to undermine the socio-economic and political stability of the state', *Man: crime and punishment,* vol. 30(1–4), iss. 3, pp. 326–335. doi : 10.33463/2687-1238.2022.30(1-4).3.326-335.

В XXI в. беспрецедентное информационное и идеологическое воздействие стран Запада и США на население Российской Федерации и ее союзников предполагает дискредитацию внешнеполитического, внешнеэкономического и внутреннего курса России. В сочетании с комплексом финансово-экономических, политико-дипломатических и санкционных мер давления на Россию происходит очевидное стирание границы между войной и мирными формами противоборства, где центр тяжести переносится в информационную плоскость. Эффективность такого сочетания подтверждается успешной реализацией технологий информационной войны при подготовке и проведении цветных революций на постсоветском пространстве и осуществлении государственных переворотов на Ближнем Востоке.

Ключевая целевая установка данных технологий в информационно-идеологическом пространстве направлена на замещение базовых традиционных ценностей общества, подрыв государственной идеологии, формирование в массовом сознании положительного образа актора-агрессора и отрицательного имиджа государственных структур. Составляющие победы в информационной войне формируются из комплекса экономических, морально-политических и технологических факторов, а также технологических возможностей для массовой сетевой коммуникации.

После 24 февраля 2022 г. для создания резко негативного образа и дискредитации России в информационном, экономическом и культурном пространстве США и европейские страны стали интенсивно использовать все доступные им ресурсы и способы, для которых характерны признаки военного периода (массированное воздействие, ожесточенность, пренебрежение нормами морали и нравственности и др.).

В 2021 г. США было выделено 590 млн долларов на противодействие влиянию Российской Федерации ($ 290 млн) и Китайской Народной Республики ($ 300 млн). По данным экспертов Лиги безопасного Интернета, за три недели проведения специальной военной операции (СВО) на информационную войну против России потрачено 270 млн долларов США. Ежедневно только на рекламу фейков и призывов к участию в незаконных акциях в Facebook и Instagram на территории РФ и Белоруссии тратится от 500 тыс. до 1,7 млн долларов США. В сравнении с рекламными системами Google данные затраты вполне сопоставимы (бюджет Google на российскую аудиторию составляет порядка $ 780 тыс. в сутки). Ежедневно на оплату труда специалистов IT-сферы, привлекаемых к информационной войне против России, выделяется 1,4 млн долларов США [11].

Активную работу по подрыву доверия к военно-политическому руководству Российской Федерации и дискредитации органов власти, а также по снижению психологической устойчивости российских военнослужащих и членов их семей ведут четыре центра информационно-психологических операций сил специальных операций Украины (ЦИПсО): 16-й ЦИПсО, с. Гуйва, Житомирская обл; 72-й ЦИПсО, г. Бровары; 74-й ЦИПсО, г. Львов; 83-й ЦИПсО, г. Одесса) [6]. Стоит отметить, что такие специализированные подразделения официально и неофициально используют многие страны. Только за 2000–2017 гг. количество киберподразделений увеличилось в 12,6 раза (рис. 1). Согласно оценке потенциала киберсферы, военных бюджетов государств, существующих стратегий кибербезопасности, нормативных документов, анализа справочной и инсайдерской информации, а также официальных комментариев лидерами по расходам на содержание кибервойск являются США, Китай, Великобритания, Южная Корея, Россия, Германия, Франция, Северная Корея, Израиль (рис. 2).

Непосредственно понятие «информационная война» как война 4-го поколения появилось в конце 1980-х годов и быстро получило широкое распространение. Так, в начале 1990-х годов появились первые теоретические, а затем и практические работы, в которых давались различные определения понятия информационной войны. В настоящее время также активно используется термин «кибервойна», который часто наделяется содержанием и значением, приписываемыми информационной войне. Первое глубокое определение термина «информационная война» было дано в докладе американской корпорации RAND «Стратегические информационные боевые действия: новое лицо войны» (Strategic Information Warfare: a New Face of War) в 1996 г. [12]. В докладе указывалось, что информационная война – это война в информационном пространстве, то есть к существующим на тот момент трем военным пространствам (су-

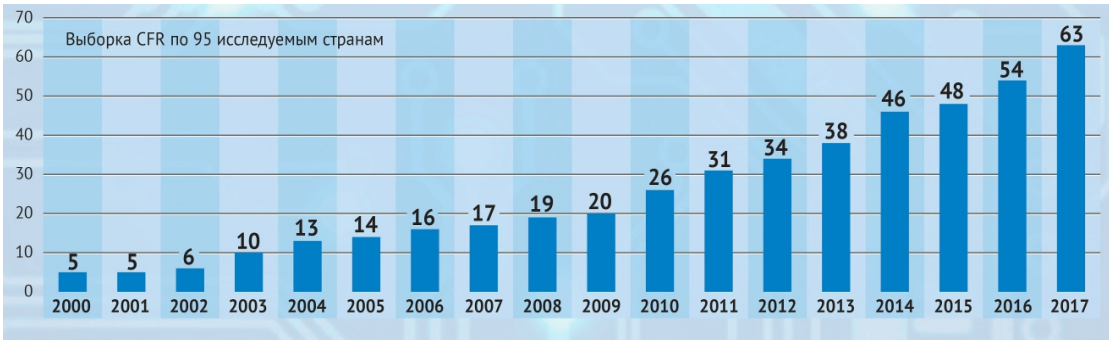

Рис. 1. Динамика изменения количества киберподразделений в военных организациях стран мира. Источник: https://ru.valdaiclub.com/multimedia/infographics/kibervoyny-bez-obyavleniya-voyny (дата обращения: 03.04.2022)

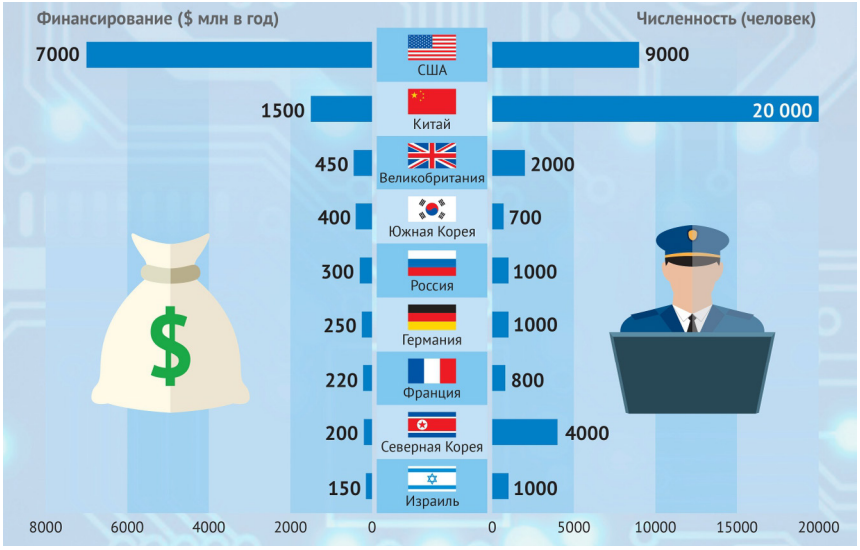

Рис. 2. Ведущие страны мира с максимальными расходами и численностью структур в сфере обеспечения специальных информационных операций. Источник: https://ru.valdaiclub.com/multimedia/infographics/kibervoyny-bez-obyavleniya-voyny (дата обращения: 03.04.2022)

хопутному, морскому и воздушному) добавилось новое – информационное пространство. Впоследствии в совместном документе, разработанном штабом Совместной доктрины информационных операций в 1998 г. [11], была дана дефиниция информационной войны, в соответствии с которой она определялась как последовательность информационных операций в рамках конфликта, в котором критически важным и стратегически дефицитным ресурсом является информация, подлежащая разработке или уничтожению.

Отметим также другие подходы к определению понятия информационной войны иностранными теоретиками. Д. Э. Деннинг (D. E. Denning) трактует информационную войну как совокупность операций, направленных на использование или эксплуатацию информационных ресурсов [14]. М. Либицкий (M. Libicki) разработал классификацию видов информационной войны:

– военное противостояние за монополизацию функций командования;
– противостояние разведки и контрразведки;
– противостояние в электронной сфере;
– психологические операции;
– организованные спонтанные хакерские атаки на информационные системы;
– информационно-экономические войны за контроль над торговлей информационными продуктами и монополизацию информации;
– кибернетические войны в виртуальном пространстве [15].

В работах современных отечественных и иностранных авторов комплексное использование возможностей электронного оружия, компьютерных сетевых операций, информационно-психологических операций, операций по военной дезинформации и дезорганизации противника, а также специальных оборонительных операций с использованием возможностей воздействия на сознание человека с целью уничтожения, морального разложения или полного перехвата влияния на процессы принятия решений противника при одновременной защите своих войск (сил) от подобного внешнего влияния определяется как информационная операция (рис. 3) [16].

В ходе информационной операции удерживается информационное превосходство и осуществляется защита собственной информации и информационных систем. Ключевой особенностью информационных операций выступает относительно «низкая стоимость создания средств информационного противоборства и информационного оружия, а соответственно – низкие финансовые и материальные затраты на проведение информационных операций» [2].

Информационные войны могут сопровождать военные действия, однако могут проводиться и отдельно. В чистом виде они предусматривают ведение войны без физического участия человека, что сводит количество жертв к минимуму. Информационной войне также присущ дистанционный характер ведения боевых действий, где объектом воздействия становится разум противника, а не просто тело, как это было в предыдущих типах войн. Само информационное оружие является оружием нелетального действия, оно приводит к поражению противника без материальных и человеческих потерь. Целью атаки становится идентичность индивида, целенаправленное изменение ее параметров. В силу этого информационная война более привлекательна, поскольку требует гораздо меньших материальных и человеческих затрат при всеобъемлющем масштабе действий.

Информационная война может вестись как внутри государства (через агентов влияния), так и на международном уровне. Массированная информационная атака часто

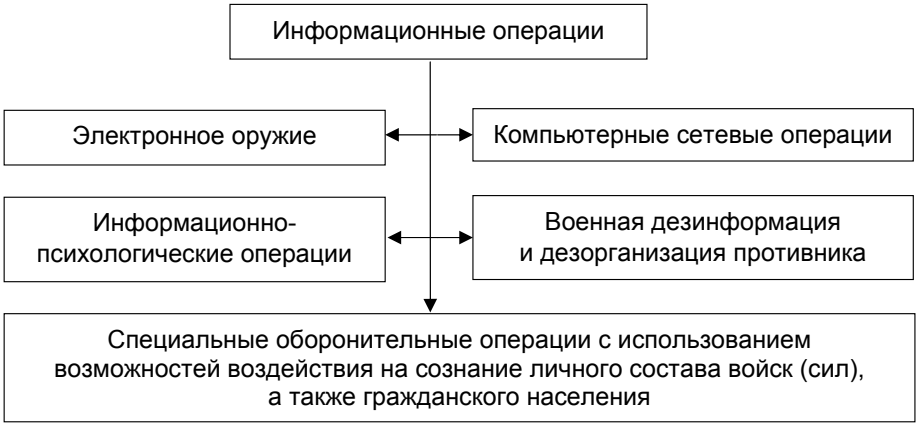

Рис. 3. Компоненты специальной информационной операции

является комбинацией внутренних и внешних операций. Эффективность информационной войны зависит от уровня организации агитации и пропаганды, основанных на чувствах и желаниях целевых социальных групп в государстве-мишени. Характерная особенность информационной войны – воздействие на общество с помощью информации. К признакам информационной войны относятся:

– ограничение доступа к определенной информации: блокирование веб-ресурсов, телевизионных программ, печатных изданий (в качестве примера следует привести блокировку аккаунтов Дональда Трампа и других лидеров Республиканской партии США в период активной фазы противостояния на выборах президента США в 2020 г. [3]; закрытие оппозиционных украинских телеканалов News One, ZIK, 112 Украина, которые активно продвигали конструктивную повестку прекращения войны на Донбассе и нормализации отношений с Российской Федерацией [9]; закрытие 16 российских телеканалов в Латвии в начале 2021 г. [7]);

– создание негативного фона по конкретным вопросам, фейковые новости и т. д. (ложная информация о наличии химического оружия в Ираке в 2003 г. [8]; телевизионные постановки ложных химических атак в Сирии в 2018 г. [5]; использование возможностей технологии дипфейк (Deepfake) для фабрикации любого видеоизображения с участием любого человека [4]);

– проникновение информации в различные сферы общества путем активного использования агентов влияния из числа лидеров общественного мнения, а также сетевых средств массовой информации, ориентированных на конкретные социальные группы [10].

Актуальные на сегодняшний день методы и инструменты ведения информационной войны были классифицированы профессором В. Ф. Байневым (рис. 4). В числе основных групп методов и инструментов были выделены киберпреступления (хакерские атаки); нагнетание страха, паники, ажиотажа, недоверия, негативных ожиданий; создание и поддержание информационной асимметрии; искажение и разрушение мировоззрения.

Таким образом, следует сформулировать вывод о том, что в информационной войне, в реальном масштабе времени, на основе сочетания финансовых, экономических, дипломатических и специальных мер осуществляется воздействие на противника и население страны. Относительно небольшие силы и средства при незначительных финансовых затратах позволяют вывести из строя военную и государственную ин-

формационную инфраструктуру. Это требует мобилизации ресурсов и всего российского общества, построения высокоэффективной и малобюджетной интегрированной системы противодействия психологическим и информационно-техническим операциям. Понимание приемов информационной войны позволяет перевести ее из разряда скрытых угроз в явные, в отношении которых необходимо применять корректирующее и предупреждающее воздействие. В свою очередь, последствия проигранного информационного противоборства приводят к гибели и эмиграции части населения страны, разрушению промышленности, потере территории, политической зависимости от агрессора, уничтожению (резкому сокращению) армии или запрету на поддержание обороноспособности, а также вывозу из страны наиболее перспективных и высоких технологий, капитала и ресурсов.

Возрастание роли компонентов информационной сферы как нового источника угрозы национальной безопасности Российской Федерации на государственном уровне в 2017 г. обозначено в Указе Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». В дальнейшем в развитие этого доктринального документа были приняты Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения,

Рис. 4. Методы и инструменты информационной войны [1]

предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Очевидно, что назрела необходимость кардинальной мобилизации сил и ресурсов Российской Федерации в отношении осуществления информационной защиты индивидуального и общественного сознания российского общества и формирования органа, отвечающего на федеральном уровне за реализацию активных мероприятий в противостоянии информационной войне. Такой подход позволит комплексно решить задачи противодействия подрывным информационным технологиям в рамках единой стратегии обеспечения национальной безопасности Российской Федерации.

Список источников

1. Байнев В. Ф. Современная информационная война как глобальный феномен // Новая экономика. 2012. № 2. С. 219–223.

2. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века : монография. СПб. : Наукоемкие технологии, 2017. 546 с.

3. В Париже не согласились с блокировкой аккаунтов Трампа в соцсетях // Интерфакс. 2021. 11 янв. URL: https://www.interfax.ru/world/744639 (дата обращения: 20.03.2022).

4. Дипфейки: что это за технология и почему она опасна // РБК. 2020. 30 сент. URL: https://trends.rbc.ru/trends/industry/5de101619a79474a179f16db (дата обращения: 20.03.2022).

5. Шимаев Р., Лушникова А., Полетаева П. «Запад плюет на законы»: как в Москве оценили заявление продюсера BBC об инсценировке «последствий химатаки» в Сирии // Rt.com. 2019. 14 февр. URL: https://russian.rt.com/world/article/602409-mid-priznanie-bbc-feik-duma (дата обращения: 22.03.2022).

6. Пережогин Е. Информационные боевики: как американского сержанта Рейеса занесло на Украину и чем он там занимается // Live.ru. 2022. 14 марта. URL: https://life.ru/p/1476607 (дата обращения: 20.03.2022).

7. Полякова В., Порываева Л. Латвия приостановит вещание еще 16 российских телеканалов // РБК. 2021. 9 февр. URL: https://www.rbc.ru/politics/09/02/2021/602282119a7947740672fed6/ (дата обращения: 20.03.2022).

8. Пауэлл представил данные спецслужб об оружии Ирака // РБК. 2003. 5 февр. URL: https://www.rbc.ru/politics/05/02/2003/5703b53c9a7947783a5a441a (дата обращения: 20.03.2022).

9. Телеканалы «112 Украина», NewsOne и ZIK прекратили вещание на Украине из-за санкций // Информационное агентство ТАСС. 2021. 3 февр. URL: https://tass.ru/mezhdunarodnaya-panorama/10609305 (дата обращения: 23.03.2022).

10. Телеграм-революции в Белоруссии не нужны лидеры. Несмотря на отсутствие четкой организации и повестки, протесты в стране продолжаются // Vtimes. 2020. 9 июля. URL: https://www.vtimes.io/2020/09/07/telegram-revolyucii-v-belorussii-ne-nuzhny-lidery-a94 (дата обращения: 23.03.2022).

11. Эксперт: сумма затрат на информационную войну против России может достигать $ 270 млн // Информационное агентство ТАСС. 2022. 16 марта. URL: https://tass.ru/ekonomika/14084339 (дата обращения: 20.03.2022).

12. Molander, R. C., Riddile, A. & Wilson, P. A. 1996, Strategic Information Warfare: a New Face of War, RAND Corporation, https://www.rand.org/pubs/monograph_reports/MR661.html.

13. Joint Pub 3-13, “Joint Doctrine for Information Operations” 1998, 9 October, http://www.c4i.org/jp3_13.pdf.

14. Denning, D. E. 1999, Information Warfare and Security. Addison-Wesley.

15. Libicki, M. C. 1995, What Is Information Warfare?, National Defense University, Institute for National Strategic Studies.

16. Information Operation Roadmap 2003, 30 October, http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_01_06_psyops.pdf.

References

1. Baynev V. F. 2012, ‘Modern information warfare as a global phenomenon’, *The New Economy*, iss. 2, pp. 219–223.

2. Makarenko, S. I. 2017, *Information warfare and electronic warfare in network-centric wars of the beginning of the XXI century: monograph*, Scientific technologies, St. Petersburg.

3. *‘In Paris they did not agree with the blocking of Trump's accounts in social networks’ 2021, Interfax,* 11 Lanuary, viewed 20 March 2022, https://www.interfax.ru/world/744639.

4. *‘Deep fakes: what kind of technology it is and why it is dangerous’* 2020, RBC, 30 September, viewed 20 March 2022, https://trends.rbc.ru/trends/industry/5de101619a79474a179f16db/.

5. Shimaev, R., Lushnikova, A. & Poletaeva, P. 2019, ‘“The West spits on the laws”: how Moscow assessed the statement of the BBC producer about the staging of the “consequences of the chemical attack" in Syria’, *Rt.com,* 14 February, viewed 20 March 2022, https://russian.rt.com/world/article/602409-mid-priznanie-bbc-feik-duma/.

6. Perezhogin, E. 2022, ‘Information fighters: how American Sergeant Reyes was brought to Ukraine and what he does there’, *Live.ru*, 14 March, viewed 20 March 2022, https://life.ru/p/1476607.

7. Polyakova, V. & Poryvaeva, L. 2021, ‘Latvia to suspend broadcasting of 16 more Russian TV channels’, *RBC*, 9 February, viewed 20 March 2022, https://www.rbc.ru/politics/09/02/2021/602282119a7947740672fed6/.

8. ‘Powell presented special services data on Iraq's weapons’ 2003, RBC, 5 February, viewed 20 March 2022, https://www.rbc.ru/politics/05/02/2003/5703b53c9a7947783a5a441a/.

9. ‘112 Ukraine, NewsOne and ZIK TV channels stopped broadcasting in Ukraine due to sanctions’ 2021, TASS News Agency, 3 February, viewed 20 March 2022, https://tass.ru/mezhdunarodnaya-panorama/10609305/.

10. ‘Telegram revolution in Belarus does not need leaders. Despite the lack of a clear organization and agenda, protests continue in the country’, 2020, *Vtimes*, 9 July, viewed 23 March 2022, https://www.vtimes.io/2020/09/07/telegram-revolyucii-v-belorussii-ne-nuzhny-lidery-a94/.

11. ‘Expert: the total cost of the information war against Russia may reach $ 270 million’ 2022, *TASS News Agency*, 16 March, viewed 20 March 2022, https://tass.ru/ekonomika/14084339.

12. Molander, R. C., Riddile, A. & Wilson, P. A. 1996, *Strategic Information Warfare: a New Face of War*, RAND Corporation, https://www.rand.org/pubs/monograph_reports/MR661.html.

13. *Joint Pub 3-13, “Joint Doctrine for Information Operations”* 1998, 9 October, http://www.c4i.org/jp3_13.pdf.

14. Denning, D. E. 1999, *Information Warfare and Security*. Addison-Wesley.

15. Libicki, M. C. 1995, *What Is Information Warfare?*, National Defense University, Institute for National Strategic Studies.

16. Information Operation Roadmap 2003, 30 October, http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_01_06_psyops.pdf.

Информация об авторах
М. Н. Козин – доктор экономических наук, профессор, главный научный сотрудник;
А. В. Родионов – доктор экономических наук, профессор кафедры экономики и менеджмента.

Information about the authors
M. N. Kozin – Sc.D (Economics), Professor, chief researcher;
A. V. Rodionov – Sc.D (Economics), professor of the department of economics and management.

Примечание
Содержание статьи соответствует научной специальности 5.2.3. Региональная и отраслевая экономика (экономические науки).

Статья поступила в редакцию 14.04.2022; одобрена после рецензирования 23.05.2022; принята к публикации 07.07.2022.
The article was submitted 14.04.2022; approved after reviewing 23.05.2022; accepted for publication 07.07.2022.