УДК 004.94 doi: 10.26102/2310-6018/2019.24.1.004

В. А. Минаев, М. П. Сычев, Л. С. Куликов, Е. В. Вайц

МОДЕЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОМУ ВЛИЯНИЮ В СОЦИАЛЬНЫХ СЕТЯХ

ФГБОУ ВО "Московский государственный технический университет им. Н. Э. Баумана", Москва, Россия

В последнее десятилетие в социальных сетях существенно усилилась деятельность как со стороны зарубежных центров, так и со стороны различных групп влияний внутри страны по организации деструктивных воздействий на российское общество и его социальные группы, особенно молодежные, с целью дестабилизации внутриполитической, социально-экономической и криминогенной обстановки. Именно поэтому в Доктрине информационной безопасности Российской Федерации информационно-психологические воздействия (ИПВ) названы важными негативными факторами, влияющими на состояние информационной безопасности (ИБ). В этой связи создание моделей противодействия деструктивным информационным воздействиям (ДИВ) манипулятивного характера в социальных сетях, оценка и прогнозирование их влияния на социальные группы выступают на современном этапе актуальными управленческими задачами. Рассмотрена системно-динамическая модель информационного противодействия ДИВ в социальных сетях. Обосновано ее применение для целей противодействия информационному терроризму, экстремизму и другим деструктивным воздействиям на современное общество посредством информационных сетей. Дано описание модели в виде потоковых диаграмм в обозначениях системной динамики. Приведены системы дифференциальных уравнений. Проведены имитационные эксперименты с моделями с применением перспективной платформы Anylogic. Модели позволяют осуществлять прогноз ДИВ с учетом фактора противодействия в социальных сетях, проигрывать различные сценарии динамики указанных взаимосвязанных процессов.

Ключевые слова: имитационное моделирование, деструктивное информационное воздействие, противодействие, управление, социальная сеть.

Введение

В новой Доктрине информационной безопасности Российской Федерации [1] указывается на расширение масштабов использования специальными зарубежными службами информационно-психологического воздействия, направленного на дестабилизацию внутриполитической, социально-экономической и криминогенной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности государств, в первую очередь, включая Россию. Направленное на размывание традиционных российских духовно-

нравственных ценностей, ДИВ ориентировано на механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в социальных сетях. Нагнетая межнациональную и социальную напряженность, разжигая этническую и религиозную вражду, пропагандируя экстремистскую идеологию, апологеты ДИВ ставят далеко идущие цели разрушения государственных устоев, перехвата управления общественными явлениями, направленными против таких устоев.

Нужно отметить, что вопросы моделирования ДИВ в социальных сетях исследованы уже во многих научных работах как в России [2-6], так и за рубежом [7-10].

В то же время, модели противодействия ДИВ исследовались явно недостаточно, хотя потребность в них становится все более актуальной. Поскольку оценка, прогнозирование и нейтрализация ДИВ в условиях все более интенсифицирующихся информационных войн разного масштаба и направленности уже не оставляет выбора для методов управления в столь противоречивой сфере. Настоящая статья развивает модели противодействия ДИВ в социальных сетях, ранее предложенные авторским коллективом [11].

Материалы и методы

В статье авторского коллектива, посвященной моделированию информационных воздействий и опубликованной в настоящем выпуске сетевого журнала, приводится обзор научных работ в указанной сфере, обосновывается создание информационно-аналитической системы мониторинга аномального поведения в регионах Российской Федерации, приводятся необходимые определения (**с**истемно-динамическое моделирование, структурные элементы имитационного моделирования уровни, темпы и др.), описание системно-динамической модели ИВ.

Построение системно-динамической модели информационного противодействия (ИПД) связано с моделью ИВ на социальные группы. Предположим на первом этапе, что в социуме одновременно идет распространение двух противоположных идей ИВ (положительной и отрицательной). Потоковая диаграмма, описывающая системно-динамическую модель ИПД, приведена на Рисунке 1, будучи представленной системой дифференциальных уравнений (1).

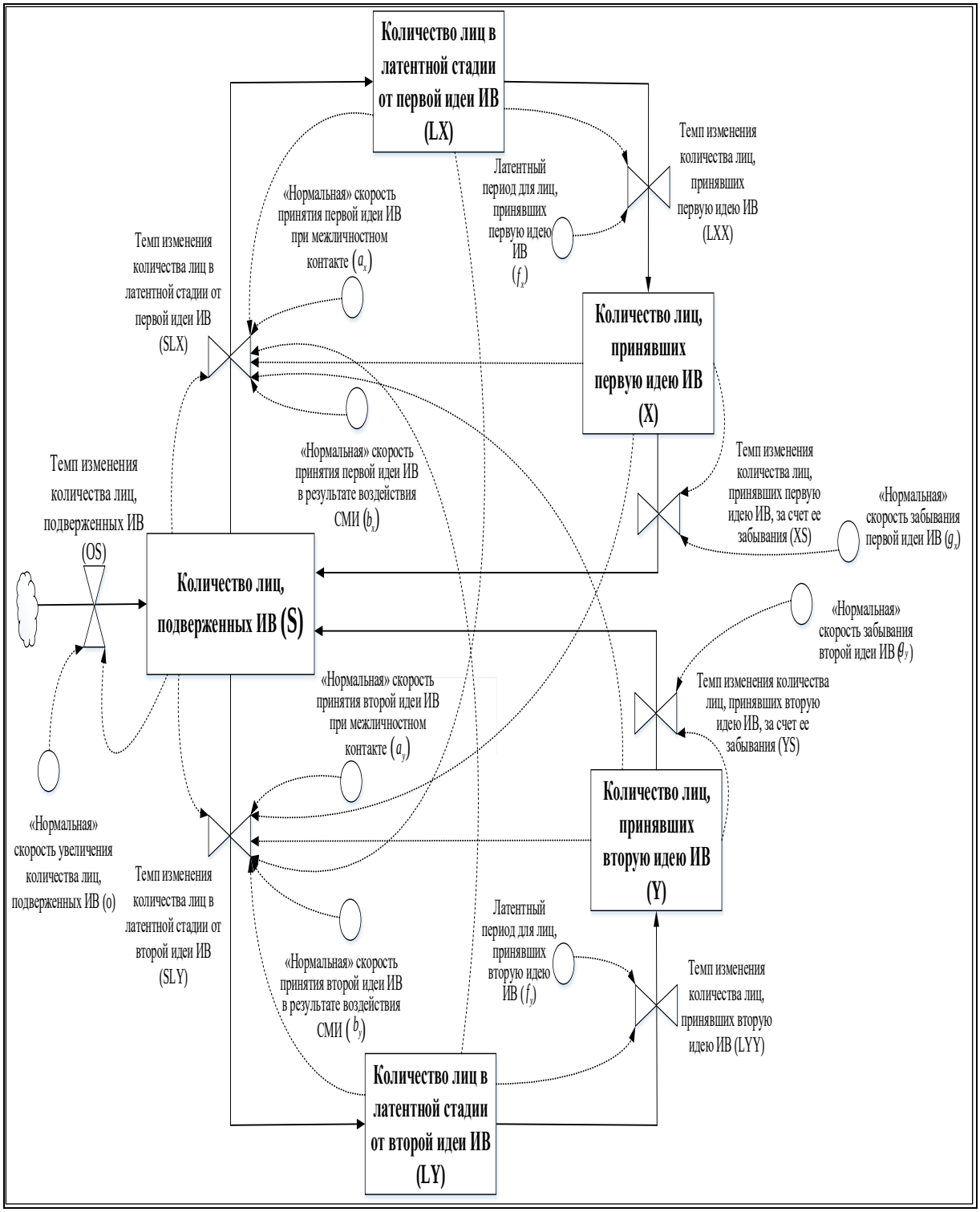

Рисунок 1 – Потоковая диаграмма системно-динамической модели ИПД

$$\begin{cases} \dfrac{dS}{dt} = OS(t) + XS(t) + YS(t) - SLX(t) - SLY(t) \\ \dfrac{dX}{dt} = LXX(t) - XS(t) \\ \dfrac{dY}{dt} = LYY(t) - YS(t) \\ SLX(t) = b_x \cdot S(t) + \dfrac{a_x \cdot S(t) \cdot X(t)}{S(t) + X(t) + Y(t) + LX(t) + LY(t)} \\ SLY(t) = b_y \cdot S(t) + \dfrac{a_y \cdot S(t) \cdot Y(t)}{S(t) + X(t) + Y(t) + LX(t) + LY(t)} \\ LXX(t) = \dfrac{LX(t)}{f_x} \\ LYY(t) = \dfrac{LY(t)}{f_y} \\ XS(t) = g_x \cdot X(t) \\ YS(t) = g_y \cdot Y(t) \\ OS(t) = o \cdot S(t) \end{cases} \quad (1)$$

Отметим, что процесс имитационного моделирования, осуществленный с использованием современной программной платформы Anylogic [12], позволяет “проигрывать” любое количество противоборствующих идей. Основными переменными, динамика которых в социуме описывалась с помощью модели ИПД, также являются количество лиц:

- подверженных ИВ;
- принявших первую – негативную идею ИВ;
- принявших вторую – позитивную идею ИВ;
- находящихся в латентной стадии от первой – негативной идеи ИВ;
- находящихся в латентной стадии от второй – негативной идеи ИВ.

При этом системно-динамическая модель ИПД, описанная в полном виде, учитывает характеристики забывания информации, существования

латентного периода, изменения размера социальной группы, топологию взаимодействия в группе, замещения идеи ИВ на идею противоборствующей стороны и другие характерные особенности.

Результаты

С моделью (1), представленной на Рисунке 1, проведен ряд имитационных экспериментов. Пример имитационного эксперимента с системно-динамической моделью ИПД приведен на Рисунке 2, на котором показана динамика количества лиц, подверженных ИВ (*S*); принявших первую – негативную (*X*) и вторую – позитивную (*Y*) идеи ИВ; а также лиц в латентной стадии от первой (*LX*) и второй (*LY*) идей ИВ.

Очевидна довольно сложная, но взаимосвязанная динамика рассматриваемых состояний, учет особенностей которой дает возможность опережающим образом предусмотреть меры по противодействию негативным информационным воздействиям в социальных сетях, особенно в периоды пиковых нагрузок.

Имитационная платформа Anylogic дает возможность более детально структурировать рассматриваемые состояния с тем, чтобы учесть более тонкие эффекты в процессе противодействия манипулятивным информационным воздействиям.

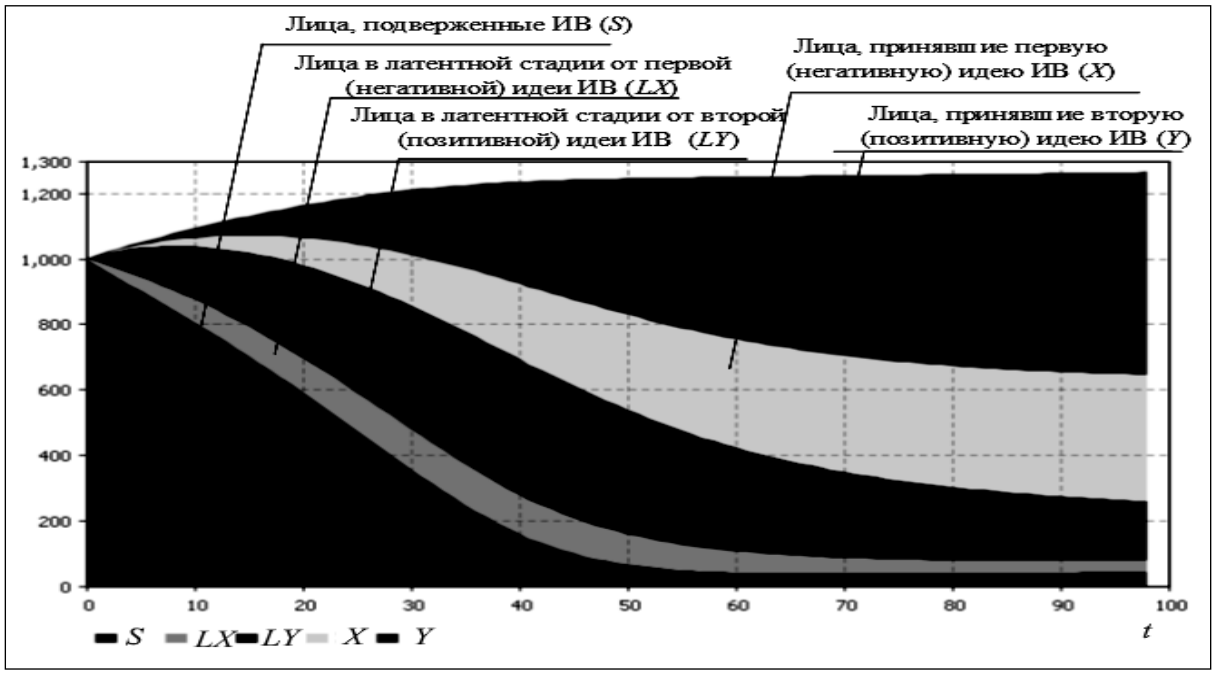

Рисунок 2 – Динамика количества лиц, подверженных ИВ (*S*), принявших первую – негативную (*X*) и вторую – позитивную (*Y*) идеи ИВ, а также лиц в латентной стадии от первой (*LX*) и второй (*LY*) идей ИВ

Обсуждение

1. Эффективность решения задач управления противодействием ДИВ может быть повышена на основе применения системно-динамического моделирования, позволяющего оценивать, анализировать и прогнозировать использование социальных сетей в качестве среды распространения идей экстремизма, терроризма, молодежной агрессии, аутоагрессии и других крайне опасных для общества явлений. Используя особую технику графического описания структур моделируемых систем – системные потоковые диаграммы, метод системной динамики позволяет в процессе управления наглядно отобразить причинно-следственные связи, а также петли обратной связи, возникающие в системе информационных воздействий.
2. Выбранная в качестве имитационной среды система Anylogic дает возможность детально проигрывать различные сценарии информационного воздействия и противодействия с использованием системно-динамической модели и визуально представлять результаты моделирования. При этом результаты имитации дают возможность заблаговременно обосновывать управленческие решения по подготовке и реализации мероприятий, направленных на снижение или нейтрализацию деструктивных ИВ на общество в целом и его социальные группы в социальных сетях, включая молодежь.
3. Системно-динамическая модель информационного противодействия, логически продолжая модели ИВ, может учитывать характеристики забывания информации, существование латентного периода, изменения размеров социальных групп, замещения идей ИВ на ряд противоположных идей. Основными переменными, динамику которых можно изучать с помощью системно-динамической модели противодействия являются: количество лиц, подверженных ИВ; количество лиц в латентной стадии от негативных и позитивных идей ИВ; количество лиц, принявших негативные и позитивные идеи ИВ.

Заключение

Итак, эффективных модельных разработок процессов деструктивных информационных воздействий и процессов противодействия им, позволяющих делать достаточно точные оценки и прогнозы в зависимости от значений и динамики различных внешних и внутренних факторов на

сегодняшний день явно недостаточно. Проведенные исследования позволяют сделать вывод о том, что для решения задачи моделирования процессов информационных воздействий на социальные группы и процессов информационного противоборства, хорошо применимы методы системно-динамического моделирования.

Разработанная в статье системно-динамическая модель информационного противодействия деструктивному информационному влиянию, воспроизводящая конкурентное взаимодействие противоположных идей в социуме, является новой, позволяя решать определенный спектр задач управления, оптимизации, прогнозирования и анализа чувствительности параметров модели.

Дальнейшим развитием данного научного направления является уточнение и детализация факторного комплекса, причинно-следственных связей и описываемых уровней в системно-динамических моделях, а также проведение дополнительной серии имитационных экспериментов с различными комбинациями факторов. А именно, планируется более углубленное исследование влияния топологических характеристик социальных сетей с целью выработки более эффективных мер со стороны региональных властей в случае манипулятивного, деструктивного влияния на социальные группы.

Перспективой развития анализа топологических различий является выявление дополнительных “глубинных” факторов, характеризующих разные поселения/города/регионы, влияющих на динамику распространения ИВ.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.
2. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. М: Издательство физико-математической литературы, 2010. – 228 с.
3. Минаев В. А., Овчинский А. С., Скрыль С. В., Тростянский С. Н. Как управлять массовым сознанием. Современные модели. М.: Издательство “Российский новый университет”, 2013. – 200 с.
4. Минаев В. А., Дворянкин С. В. Моделирование динамики информационно-психологических воздействий на массовое сознание // Вопросы кибербезопасности. 2016. № 5 (18). – С. 56-64.
5. Минаев В. А., Дворянкин С. В. Обоснование и описание модели динамики информационно-психологических воздействий

деструктивного характера в социальных сетях // Безопасность информационных технологий. 2016. Том 23. № 3. – С. 40-52.
6. Минаев В. А., Сычев М. П., Вайц Е. В., Грачева Ю. В. Моделирование угроз информационной безопасности с использованием принципов системной динамики // Вопросы радиоэлектроники. 2017. № 6. – С. 75-82.
7. Cappelli D. M., Desai A. G., Moore A. P., Shimeall T. J., Weaver E. A., Bradford B. J. Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage. Pittsburg: Carnegie Mellon University. Software Engineering Institute, 2006. – 34 p.
8. Behara R. S., Derrick Huang C. A. System Dynamics Model of Information Security Investments // Journal of Information System Security. 2010. Vol. 6. No. 2. – Pp. 1572-1583.
9. Kim A. C., Lee S. M., Lee D. H. Compliance Risk Assessment Measures of Financial Information Security Using System Dynamics // International Journal of Security and Its Applications. 2012. Vol. 6. No. 4. – Pp. 191-200.
10. Liu W., Cui Y., Li. Y. Information Systems Security Assessment Based on System Dynamics // International Journal of Security and Its Applications. 2015. Vol. 9. No. 2. – Pp. 73-84.
11. Минаев В. А., Сычев М. П., Вайц Е. В., Киракосян А. Э. Системно-динамическое моделирование информационных воздействий на социум // Вопросы радиоэлектроники. 2017. № 11. – С. 35-43.
12. Маликов Р. Ф. Практикум по имитационному моделированию сложных систем в среде AnyLogic 6: учебное пособие. Уфа: Изд-во БГПУ, 2013. – 296 с.

V.A. Minaev, M.P. Sychev, L.S. Kulikov, E.V. Vaitz

MODELING OF COUNTERACTION TO DESTRUCTIVE INFLUENCE IN SOCIAL NETWORKS

Bauman Moscow State Technical University, Moscow, Russia

In the last decade, the activity of both foreign centers and various groups of influences within the country on the organization of destructive impacts on Russian society and its social groups, especially youth, in order to destabilize the domestic political, socio-economic and criminal situation has significantly increased in social networks. That is why in the Doctrine of information security of the Russian Federation information and psychological effects (IPE) are called important negative factors affecting the state of information security (IS). In this regard, the creation of models to counter destructive information impacts (DII) of manipulative

nature in social networks, assessment and forecasting of their impact on social groups are at the present stage actual management tasks. The system-dynamic model of information counteraction of DII in social networks is considered. Its application for the purposes of counteraction to information terrorism, extremism and other destructive influences on modern society by means of information networks is proved. The description of the model in the form of flowcharts in the designations of system dynamics is given. Systems of differential equations are shown. Simulation experiments with models using the promising Anylogic platform were carried out. The model make it possible to forecast DII taking into account the factor of counteraction in social networks, to play different scenarios of the dynamics of these interrelated processes.

Keywords: simulation modeling, destructive information impact, counteraction, management, social network.

REFERENCES

1. The Doctrine of information security of the Russian Federation. Approved by the decree of the President of the Russian Federation. No. 646 of December 5, 2016. (In Russ.)
2. Gubanov D. A., Novikov D. A., Chkhartishvili A. G. [Social networks: models of information influence, management and confrontations]. M: Publishing house of physical and mathematical literature, 2010. – 228 p. (In Russ.)
3. Minaev V. A., Ovchinskij A. S., Skryl' S. V., Trostyanskij S. N. [How to manage mass consciousness. Modern models]. M.: Publishing House "Russian New University", 2013. – 200 p. (In Russ.)
4. Minaev V. A., Dvoryankin S. V. [Modeling dynamics of informational-psychological influences on mass consciousness] // Voprosy kiberbezopasnosti = Cybersecurity issues. 2016. № 5 (18). - Pp. 56-64. (In Russ.)
5. Minaev V. A., Dvoryankin S. V. [Rationale and description of dynamics model of informational-psychological impacts of a destructive nature in social networks] // Security of information technologies. 2016. Vol. 23. No. 3. – Pp. 40-52. 2016. (In Russ.)
6. Minaev V. A., Sychev M. P., Vaitz E. V., Gracheva YU. V. [Modeling of information security threats using the principles of system dynamics // Voprosy radioehlektroniki = Problems of Radio Electronics. 2017. No. 6. - Pp. 75-82. (In Russ.)
7. Cappelli D. M., Desai A. G., Moore A. P., Shimeall T. J., Weaver E. A., Bradford B. J. Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage. Pittsburg: Carnegie Mellon University. Software Engineering Institute, 2006. – 34 p.

8. Behara R. S., Derrick Huang C. A. System Dynamics Model of Information Security Investments // Journal of Information System Security. 2010. Vol. 6. No. 2. – Pp. 1572-1583
9. Kim A. C., Lee S. M., Lee D. H. Compliance Risk Assessment Measures of Financial Information Security Using System Dynamics // International Journal of Security and Its Applications. 2012. Vol. 6. No. 4. – Pp. 191-200.
10. Liu W., Cui Y., Li. Y. Information Systems Security Assessment Based on System Dynamics // International Journal of Security and Its Applications. 2015. Vol. 9. No. 2. – Pp. 73-84.
11. Minaev V. A., Sychev M. P., Vaitz E. V., Kirakosyan A. E. [System-dynamics modeling information influences of on society] // Voprosy radioehlektroniki = Problems of Radio Electronics. 2017. No. 11. – Pp. 35-43. (In Russ.)
12. Malikov R. F. [A training manual on simulation of complex systems in AnyLogic]. Ufa: Publishing House of Bashkir State Pedagogical University, 2013. – 296 p. (In Russ.)