УДК 004.94 doi:10.26102/23106018/2019.24.1.003

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

МОДЕЛИРОВАНИЕ МАНИПУЛЯТИВНЫХ ВОЗДЕЙСТВИЙ В СОЦИАЛЬНЫХ СЕТЯХ

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

В Доктрине информационной безопасности Российской Федерации основными негативными факторами, влияющими на состояние информационной безопасности (ИБ), называются информационно-технические (ИТВ) и информационно-психологические воздействия (ИПВ). Поэтому моделирование, оценка и прогнозирование манипулятивных информационных воздействий (МИВ) на социальные группы является актуальной задачей управления. Рассмотрены системно-динамические модели информационных воздействий в социальных сетях и группах. Обосновано их применение для целей противодействия информационному терроризму и экстремизму. Дано описание в виде потоковых диаграмм в обозначениях системной динамики. Приведены системы дифференциальных уравнений. Проведены эксперименты с моделями с применением перспективной имитационной платформы Anylogic. В результате сравнения агентной и системно-динамической моделей выявлено их высокое согласование между собой и со статистическими данными. Применяя кластерный анализ, в выборочной совокупности российских поселений выделены однородные типологические группы, различающиеся средним временем распространения информационных воздействий. Впервые был применен постулат Гиббса для изучения распространения информационных воздействий в студенческой среде. В проведенных экспериментах на реальных статистических данных выявлена высокая согласованность результатов моделирования с эмпирическими данными (коэффициенты детерминации не менее 90%). Модели позволяют осуществлять прогноз ИВ, проигрывать различные сценарии динамики указанных процессов.

Ключевые слова: имитационное моделирование, информационное воздействие, управление, социальная сеть, топология, типология, кластерный анализ.

Введение

Среди негативных факторов, влияющих на состояние информационной безопасности нашей страны, в новой Доктрине информационной безопасности Российской Федерации основными называются информационно-технические (ИТВ) и информационно-психологические воздействия (ИПВ) [1].

Так, в Доктрине отмечается, что рядом зарубежных стран производится наращивание информационно-технического воздействия (ИТВ) на информационную инфраструктуру российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса. Возрастают масштабы компьютерной преступности в кредитно-

финансовой сфере, увеличивается число преступлений при обработке персональных данных, связанных с неприкосновенностью частной жизни, личной и семейной тайны.

В Доктрине прямо указывается на интенсификацию использования специальными зарубежными службами мер по дестабилизации внутриполитической и социально-экономической обстановки во многих странах мира, и Россия не является здесь исключением.

Как отмечено в Доктрине:

- наращивается информационное давление на российское население, в первую очередь, на молодежь, направленное на размывание традиционных духовно-нравственных ценностей;
- с целью нагнетания межнациональной и социальной напряженности в российском обществе, разжигания этнической и религиозной вражды, распространения экстремистской идеологии террористические и экстремистские организации расширяют поле информационного воздействия на индивидуальное, групповое и общественное сознание.

К настоящему времени актуализировались и стали интенсивно осуществляться исследования в области анализа, моделирования и прогнозирования негативных информационных воздействий (ИВ) и информационно-психологических противодействий (ИПД) им [2-5].

Появились современные научные работы, отражающие распространение таких воздействий с помощью компьютерных сетей в различных социальных средах (школьных, студенческих, фанатских и иных), различных поселениях (мегаполисах с их специфическими малыми группами, несущими опасность для молодых людей – группы самоубийц, этнические криминальные группы, руферы, диггеры, зацеперы в метро и др., малых и моногородах - с тотальной безработицей и аморальными образцами поведения среди взрослых) [6].

Вышеизложенное позволяет заключить, что моделирование, оценка и прогнозирование манипулятивных информационных воздействий (МИВ) на социальные группы являются актуальными задачами управления.

Материалы и методы

Для количественно-качественного исследования информационного “заражения” социальных групп российского общества к сегодняшнему дню уже создана серьезная научная база в сфере моделирования информационных воздействий на социальные группы, позволяющая изучать влияние на этот процесс различных внешних и внутренних

факторов [2–6]. Указанную базу составляют различные типы: топологические, факторные, регрессионные, вероятностные и другие, составляющие основу для дальнейшего совершенствования инструментария моделирования в сфере манипулятивного информационного воздействия на социум.

Вместе с тем, наиболее эффективные с практической точки зрения имитационные методы моделирования информационных воздействий, позволяющие проигрывать различные сценарии поведения социальных групп, учитывать при этом сложное сочетание факторного комплекса, пока в нашей стране недостаточно развиты.

Исходя из изложенного, выделяются два важных направления разработки моделей, связанных с ИТВ, с одной стороны, и с ИПВ – с другой. Кроме того, процесс моделирования был бы неполон, если бы не рассматривались модели противодействия ИТВ и ИПВ. В Таблице 1 показана степень разработанности названных моделей, оцененная авторами в ходе экспертного опроса по 10-ти балльной шкале (в нем участвовали 45 квалифицированных экспертов).

Таблица 1 - Степень разработанности моделей информационных воздействий

Модели информационных воздействий	Модели ИТВ	Модели противодействия ИТВ	Модели ИПВ	Модели противодействия ИПВ
Степень разработанности моделей (баллы)	**7**	**5**	**5**	**3**

В настоящей статье рассмотрена базовая модель ИПВ (как слабо разработанная) и некоторые результаты ее применения. В ней созданы и реализованы математические модели, позволяющие имитировать ИПВ в социальных сетях и при непосредственном общении индивидов в разнообразных общественных группах. При этом применялась перспективная программная платформа имитационного моделирования Anylogic, на основе которой реализованы модели с высокими коэффициентами объясняемости (не менее 90%) между эмпирическими и модельными данными [7].

Созданная методологическая и методическая база позволяет расширить поле исследований информационных воздействий и создания моделей информационных взаимодействий при проявлениях экстремизма, терроризма и агрессивного поведения социальных групп, включая обучающихся в образовательных организациях.

Для решения последней из названных задач необходимо:

- обосновать и построить базу данных, позволяющую по сетевому информационному контенту распознавать и визуализировать ситуации возникновения агрессивного поведения тех или иных групп населения. К настоящему времени разработаны современные методы анализа контента, позволяющие выявлять инициаторов такого контента и сетевые узлы, которые с инициаторами связаны;
- изучить и спрогнозировать динамику “заражения” обучающихся стереотипами агрессивного поведения. Для этого целесообразно комплексно использовать методы системно-динамического, агентного и дискретно-событийного моделирования [8];
- создать распределенную информационно-аналитическую систему (ИАС) мониторинга агрессивного поведения в регионах Российской Федерации, с введением в указанной системе региональных ситуационных центров, где бы происходила оперативная обработка информации и принятие специалистами решений по возникающим случаям “экстремального напряжения” в социальной среде, включая ее молодежную часть.

По сути, речь идет о построении глобальной информационной системы мониторинга в масштабах страны, которая дает возможность:

- своего развития путем включения в нее (по мере готовности и необходимости) модулей мониторинга проявлений экстремизма, терроризма и других социально опасных явлений, а также модулей подготовки управленческих решений для региональных органов власти при реагировании на подобные явления и ситуации;
- использования перспективных программно-математических средств и методов при реализации механизмов комплексного реагирования на проявления агрессивного поведения;
- надежной защиты центров информационного доступа и коммуникационных каналов ИАС.

Учитывая масштабность и острую социальную необходимость реализации на современном уровне механизмов комплексного реагирования на проявления агрессивного и аномального поведения (эта проблема, исходя из мировых трендов, может только усиливаться), создание высокоорганизованной ИАС связано с привлечением для ее развития высокопрофессиональных специалистов из разных сфер деятельности (математиков, психологов, педагогов, психиатров, представителей из информационной сферы, из области защиты информации и других).

Приведем необходимые определения, относящиеся к предмету, цели и задачам настоящей статьи.

Системно-динамическое моделирование – это *метод моделирования и имитации сложных динамических систем, характеризующихся разветвленными, как правило, нелинейными связями* [9]. Системная динамика, как новое направление в области моделирования, получила свое развитие, благодаря:

- успехам в области анализа и проектирования сложных систем управления;
- прогрессу в сфере компьютерного моделирования и вычислительных методов.

Базовые работы в этом направлении относятся к исследованиям Дж. Форрестера конца 50-х – начала 60-х прошлого столетия, посвященных анализу промышленных предприятий [10], развитию городов [11] и мировой динамике [12].

За рубежом созданием системно-динамических моделей в области информационной безопасности занимаются многие научные коллективы. Достаточно назвать Университет Карнеги – Меллона и Флоридский Атлантический университет, США [13, 16], Оборонный научно-технический университет НОА, КНР [14], Высшая школа информационной безопасности, Южная Корея [15] и другие научные центры мира.

Созданные за рубежом модели успешно применяются на практике, однако требуют концептуальной и методической доработки и дополнительных исследований для того, чтобы решать задач анализа, оценки, прогнозирования и управления в сфере манипулятивных информационных воздействий.

В основе моделей системной динамики лежат общие структурные элементы, пригодные для моделирования многих систем [10-12]:

- ***уровни*** – управляемые объекты, отображаемые переменными, значения которых представляют интегральные характеристики состояний реальных потоков, рассматриваемых в моделируемой системе;
- ***темпы*** – скорости потоков, исходящих от одних уровней и входящих в другие, вызывая в них соответствующие изменения.

Кроме того, в моделях используются ***функции решений,*** **определяемые через** функциональные зависимости, существующие в системе; ***вспомогательные величины и константы.***

Системная динамика, представляя собой определенную целостность принципов и методов анализа динамических управляемых систем с

обратной связью, дает возможность их применения для решения многих организационно-производственных и социально-экономических задач.

Метод системной динамики предполагает, что для основных фазовых переменных (*системных уровней*) используются дифференциальные уравнения типа [17]:

$$\dot{y} = y^{+} - y^{-} \quad (1)$$

где $\dot{y}$ – производная переменной y по времени;

y+ – комплекс факторов, положительно сказывающихся на скорости изменения уровня y;

y– – комплекс факторов, отрицательно сказывающихся на скорости изменения уровня y.

В моделях Форрестера предполагается, что y±, в свою очередь, являются функциями уровней.

$$y^{\pm} = f(F_1, F_2, \ldots, F_k), \quad (2)$$

где k – количество факторов, меньшее числа фазовых переменных, каждый из которых зависит только от части системных уровней.

На Рисунке 1 приведено описание системно-динамической модели МИВ с обозначениями, рассматриваемыми в системе дифференциальных уравнений (3).

$$\begin{cases} \frac{dS}{dt} = OS(t) + YS(t) - SL(t) \\ \frac{dY}{dt} = SL(t) - LY(t) \\ \frac{dR}{dt} = LY(t) - YR(t) - YS(t) \\ OS(t) = o \cdot S(t) \\ SL(t) = b \cdot S(t) + \frac{a \cdot T \cdot S(t) \cdot Y(t)}{S(t) + Y(t) + L(t) + R(t)} \\ YR(t) = c \cdot Y(t) \\ LY(t) = \frac{L(t)}{f} \\ YS(t) = g \cdot Y(t) \\ a = p \cdot k_0 \cdot n \\ b = M \cdot k_1 \cdot k_2 \end{cases} \quad (3)$$

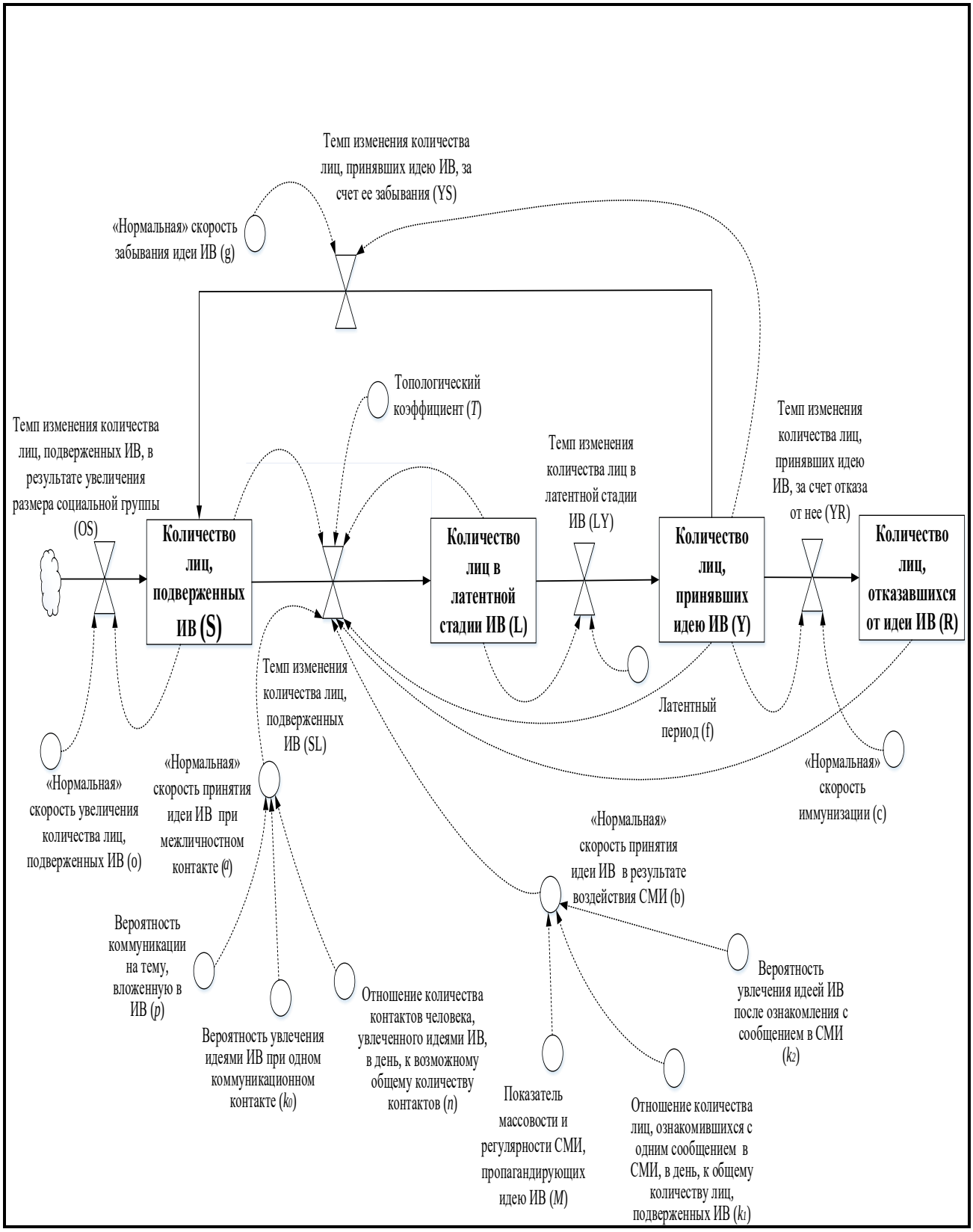
Темп изменения количества лиц, принявших идею ИВ, за счет ее забывания (YS)
«Нормальная» скорость забывания идеи ИВ (g)
Топологический коэффициент (T)
Темп изменения количества лиц, подверженных ИВ, в результате увеличения размера социальной группы (OS)
Количество лиц, подверженных ИВ (S)
Количество лиц в латентной стадии ИВ (L)
Темп изменения количества лиц в латентной стадии ИВ (LY)
Количество лиц, принявших идею ИВ (Y)
Темп изменения количества лиц, принявших идею ИВ, за счет отказа от нее (YR)
Количество лиц, отказавшихся от идеи ИВ (R)
Темп изменения количества лиц, подверженных ИВ (SL)
Латентный период (f)
«Нормальная» скорость увеличения количества лиц, подверженных ИВ (o)
«Нормальная» скорость принятия идеи ИВ при межличностном контакте (a)
«Нормальная» скорость иммунизации (c)
«Нормальная» скорость принятия идеи ИВ в результате воздействия СМИ (b)
Вероятность коммуникации на тему, вложенную в ИВ (p)
Вероятность увлечения идеями ИВ при одном коммуникационном контакте (k_0)
Отношение количества контактов человека, увлеченного идеями ИВ, в день, к возможному общему количеству контактов (n)
Вероятность увлечения идеей ИВ после ознакомления с сообщением в СМИ (k_2)
Показатель массовости и регулярности СМИ, пропагандирующих идею ИВ (M)
Отношение количества лиц, ознакомившихся с одним сообщением в СМИ, в день, к общему количеству лиц, подверженных ИВ (k_1)

Рисунок 1- Системная потоковая диаграмма системно-динамической модели МИВ

Для практической реализации системно-динамической модели МИВ использовались статистические данные о распространении различных информационных воздействий в социальных сетях, а также данные опросов в социальных группах. Основными переменными, динамика которых в исследуемом социуме анализировалась с помощью разработанной модели, являются количество лиц:

- подверженных ИВ;
- находящихся в латентной стадии ИВ;
- принявших идею ИВ;
- отказавшихся от идеи ИВ.

Результаты моделирования

Результаты модельных экспериментов по изучению влияния различных параметров на динамику процессов МИВ приведены на Рисунках 2 – 4.

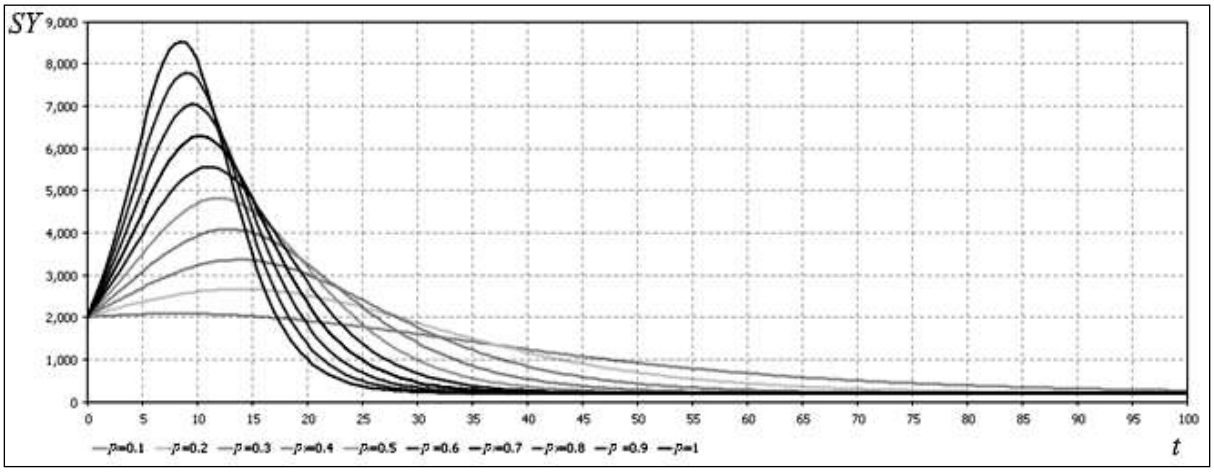

Рисунок 2 – Изменение скорости ИВ (SY) в зависимости от вероятности коммуникации на тему, вложенную в контент ИВ (p)

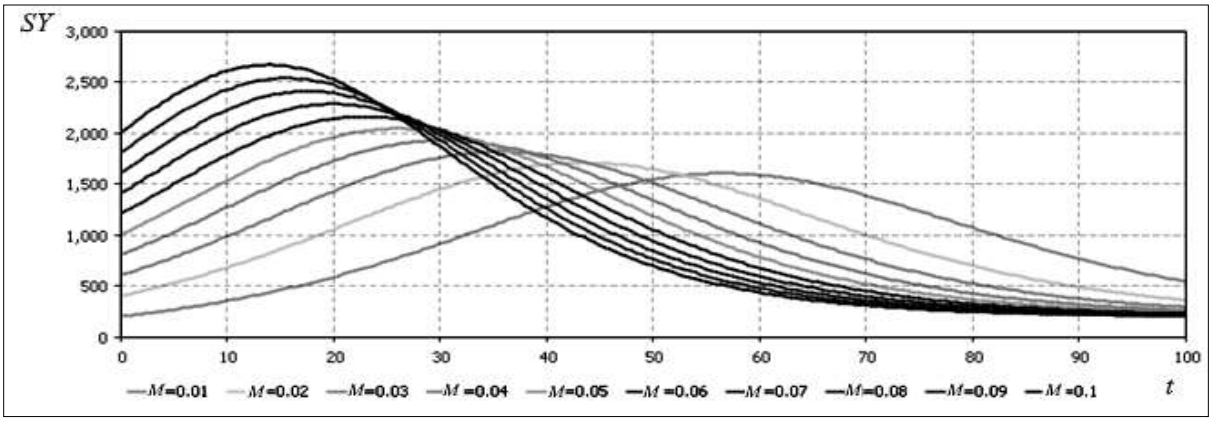

Рисунок 3 – Изменение скорости ИВ (SY) в зависимости от показателя массовости и регулярности СМИ, пропагандирующих идею ИВ (M)

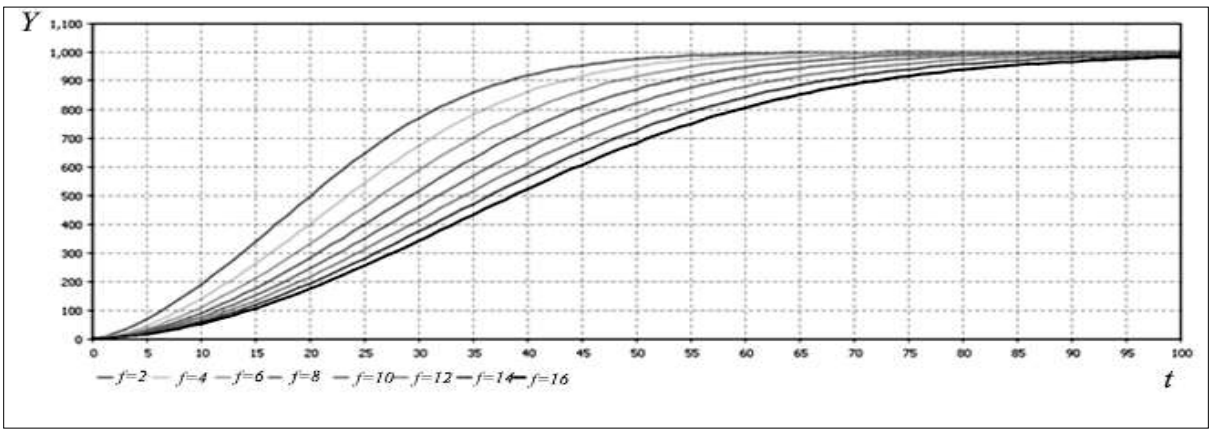

Рисунок 4 - Динамика принявших идею ИВ (Y),
в зависимости от длительности латентного периода (f)

Отметим, что результаты моделирования на основе системно-динамического и агентного подходов совпали с достаточной степенью точности (Рисунок 5). Коэффициент согласования между моделями составил 94%, со статистическими данными – 92 %.

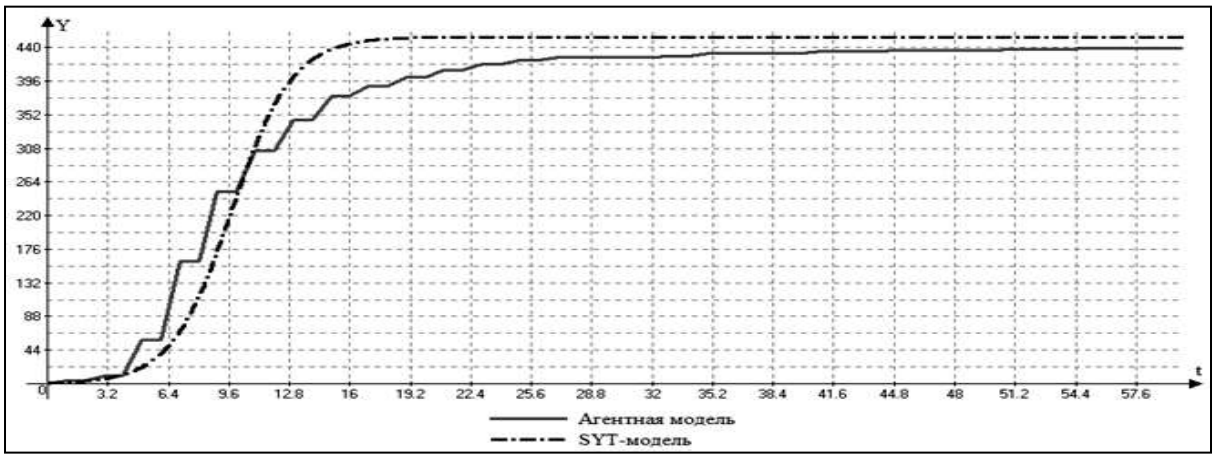

Рисунок 5 – Результаты сравнительного моделирования ИВ на основе системно-динамического и агентного подходов

В экспериментах на фактических статистических данных имитировалось по отдельности распространение ИВ от семи различных пользователей, а также одновременно с нескольких узлов социальной сети (Рисунок 6).

Из Рисунка 6 следует, что динамика количества лиц, “зараженных” идей ИВ, в зависимости от источника “заражения” в г. К. различается, подчиняясь общим динамическим закономерностях логистического характера.

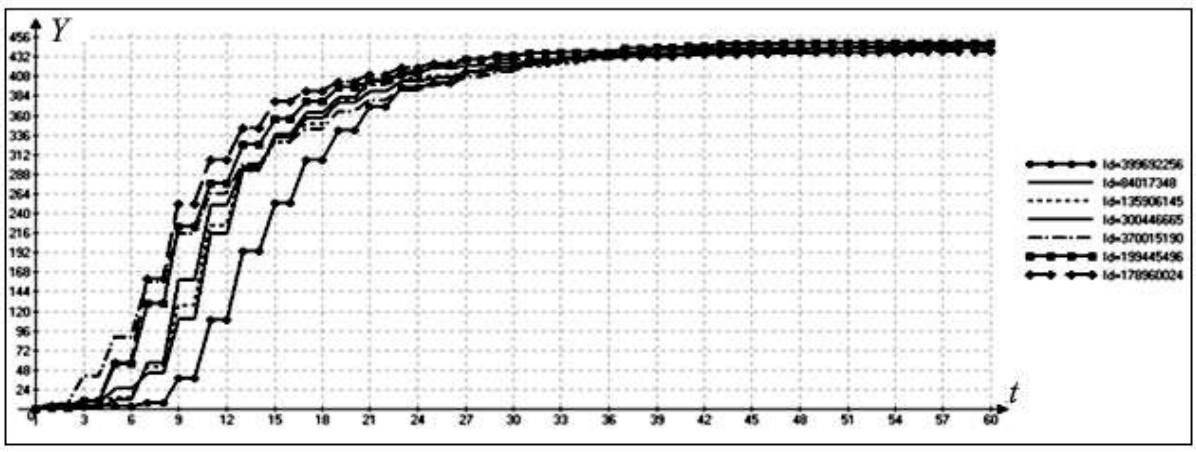

Рисунок 6 - Динамика количества лиц, “зараженных” идей ИВ, в зависимости от источника “заражения” в г. К.

Далее для расширения эксперимента в качестве объектов исследования выбраны 42 поселения России с числом жителей 10 – 20 тыс. человек. По реальным данным построен граф сетевых связей между пользователями социальной сети “ВКонтакте”, а также рассчитаны ее топологические характеристики: коэффициент кластеризации, степень связности, диаметр, плотность, средняя длина пути.

Для выделения однородных групп поселений, исходя из топологических характеристик, применен иерархический метод кластерного анализа – метод Вальда. Дендрограмма кластеризации представлена на Рисунке 7: выделены четыре кластера и один индивидуальный объект, различающиеся временем распространения ИВ в них.

В Таблице 2 показано среднее время распространения ИВ в различных кластерах. Её анализ показывает, что наблюдается существенное различие среднего времени распространения ИВ в кластерах.

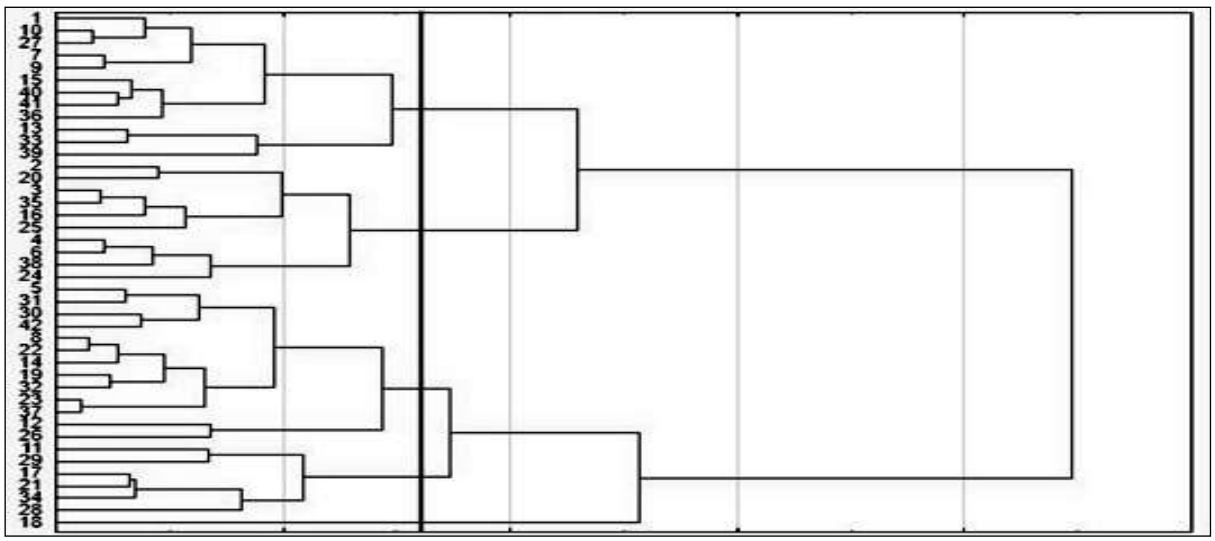

Рисунок 7 - Типологические группы выборочной совокупности поселений России

Таблица 2 - Среднее время распространения ИВ в кластерах

№ кластера	Среднее время распространения идеи ИВ, часы
1-й кластер	**310**
2-й кластер	**250,4**
3-й кластер	**181**
4-й кластер	**133,25**
Индивидуальный объект	**62**

Данное обстоятельство требует различной стратегии и тактики со стороны соответствующих государственных структур по организации информационного противодействия МИВ в поселениях, относящихся к различным типологическим группам. Это в полной мере относится к сфере борьбы с терроризмом и экстремизмом в информационной сфере.

Системно-динамическая модель (3) была апробирована на статистических данных по сообществу в социальной сети “ВКонтакте”, созданному для организации политического митинга с экстремистскими лозунгами.

Динамические зависимости, полученные по результатам моделирования, показывают высокую объясняемость модели, коэффициент детерминации равен 95% (Рисунок 8). Отметим, что в динамике распространения ИВ о проведении оппозиционного митинга выделяются два периода с разными параметрами модели ИВ, соответствующими двум информационным вбросам, произошедшим в российских городах в тот период.

В статистической физике используется известный постулат Гиббса об ансамблях [18]. Существо постулата в том, что независимые параллельные процессы в различных однородных статистических системах протекают со схожей динамикой и параметрами. Авторами была выдвинута гипотеза о том, что и в однородных независимых популяциях процессы информационного воздействия также схожи, описываясь одной и той же моделью с одинаковыми параметрами.

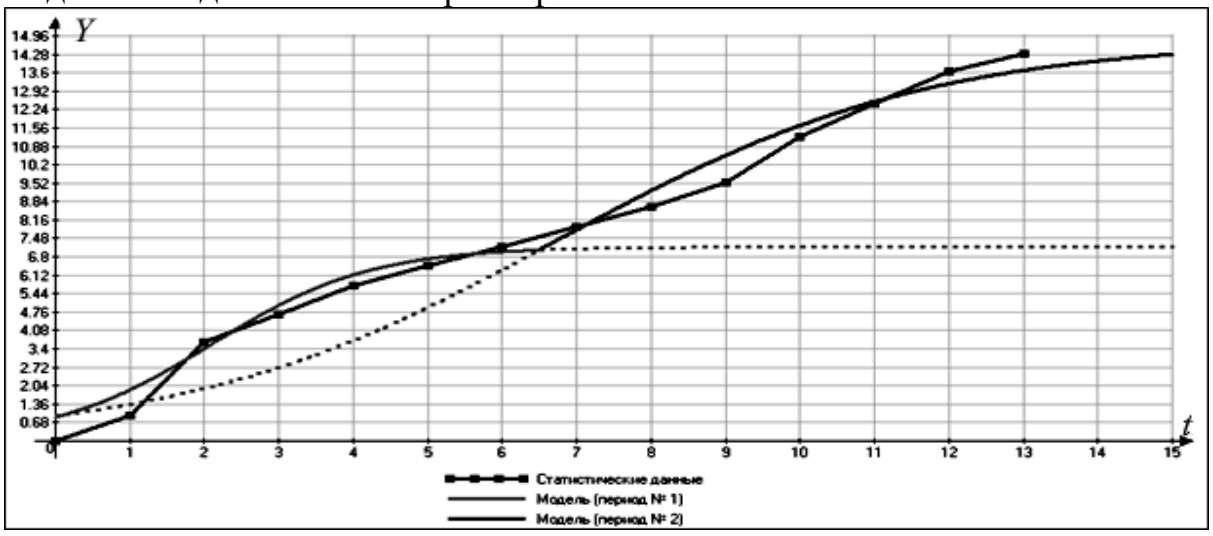

Рисунок 8 - Моделирование динамики распространения в социальной сети ИВ о проведении оппозиционных митингов

Эксперимент по распространению идеи ИВ проводился в студенческой среде (Рисунок 9). В качестве объектов для распространения идеи ИВ

выбраны семь независимых студенческих групп, обучающихся в различных вузах медицинского профиля. Вероятность контакта между участниками групп принималась равной нулю в силу автономной организации образовательного процесса.

Итак, проведенные эксперименты показали, что системно-динамические модели информационного воздействия подтвердили их эффективность и работоспособность при анализе, оценке и прогнозировании распространения ИВ в зависимости от скорости информационного “заражения”, особенностей социальных групп, топологии социальных сетей и других факторов.

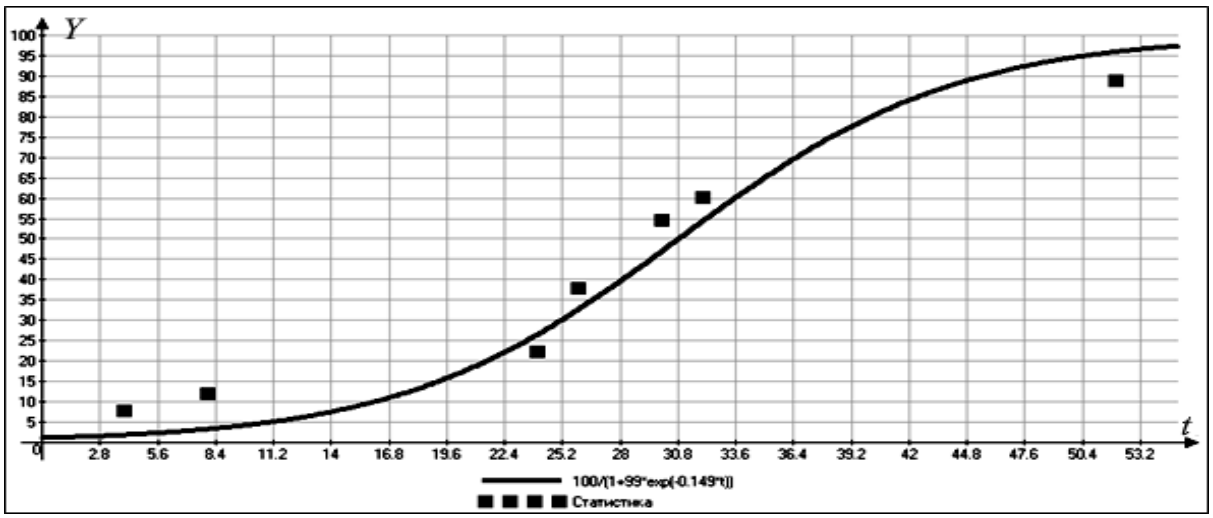

Рисунок 9 - Результаты эксперимента по распространению ИВ в студенческой среде

Выводы

1. Для решения задач исследования негативных ИВ на социальные группы, а также управления этими процессами эффективно применение методов системно-динамического и агентного моделирования, используемого на сегодняшний день для исследования различных сложных социально-экономических процессов.
2. Имитационные модели ИВ позволяют оценивать, анализировать и прогнозировать использование социальных сетей в качестве среды распространения экстремизма, терроризма, молодежной агрессии, аутоагрессии и других крайне опасных явлений.
3. Результаты расчетов с помощью системы уравнений, реализованной в имитационной системе Anylogic, дают возможность территориальным органам управления структурам заблаговременно обосновывать управленческие решения по подготовке и реализации мероприятий, направленных на снижение или нейтрализацию указанных негативных

ИВ на общество в целом и его социальные группы в социальных сетях, включая молодежь.

4. Программное обеспечение современных имитационных систем дает возможность детально проигрывать различные сценарии с использованием системно-динамических и агентных моделей, наглядно интерпретировать результаты моделирования.
5. Топологические различия социальных сетей, используемых в качестве современной среды ИВ, могут эффективно использоваться для построения стратегии и тактики информационного контакта с населением со стороны региональных властей и обоснования системы противодействия негативным информационным влияниям на социальные группы, особенно – на молодежные.
6. Новым, пока не использованном нигде в моделях информационных воздействий, выступает подход с применением для социальных процессов постулата Гиббса из статистической физики.
7. Перспектива развития топологического анализа различий в рамках системно-динамического подхода связана с выявлением дополнительных «глубинных» факторов, характеризующих разные поселения/города/регионы, влияющих на динамику распространения идеи ИВ.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.
2. 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.
3. Минаев В. А., Дворянкин С. В. Моделирование динамики информационно-психологических воздействий на массовое сознание // Вопросы кибербезопасности. 2016. № 5 (18). – С. 56-64.
4. Минаев В. А., Дворянкин С. В. Обоснование и описание модели динамики информационно-психологических воздействий деструктивного характера в социальных сетях // Безопасность информационных технологий. 2016. Т.23. № 3. – С. 40-52.
5. 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.

6. 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.
7. 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.
8. Маликов Р. Ф. Практикум по имитационному моделированию сложных систем в среде AnyLogic 6: учебное пособие. Уфа: Изд-во БГПУ, 2013. – 296 с.
9. Алехнович С.О., Слизовский Д.Е., Ожиганов Э.Н. Системно-динамическое моделирование: принципы, структура и переменные (на примере Московской области) // Вестник РУДН. Серия “Политология”. 2009, № 1. – С. 22-36.
10. Форрестер Дж. Основы кибернетики предприятия (индустриальная динамика). М.: Прогресс, 1971. – 340 с.
11. Форрестер Дж. Динамика развития города. М.: Прогресс, 1974. – 281 с.
12. Форрестер Дж. Мировая динамика. М.: Наука, 1978. – 384 с.
13. 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.
14. 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.
15. 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.
16. 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.
17. Гусаров А. Н., Жуков, Д. О., Косарев, А. В. Описание динамики распространения компьютерных угроз в информационно-вычислительных сетях с запаздыванием действия антивирусов // Вестник МГТУ им. Н.Э. Баумана. Сер. “Приборостроение”. 2010. №1. – С. 112-120.
18. Гиббс Дж. Основные принципы статистической механики / пер. с англ. К. В. Никольского. М.-Л.: Гостехиздат, 1946. – 203 с.

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

MODELING MANIPULATIVE INFLUENCES IN SOCIAL NETWORKS

Bauman Moscow State Technical University, Moscow, Russia

In the Doctrine of information security of the Russian Federation the main negative factors affecting the state of information security (IS), called informational and technical influences (ITI) and information and psychological influences (IPI). Therefore, modeling, evaluation and forecasting of information influences (II) on social groups and organizing of the corresponding information counteraction (ICA) are urgent tasks of management. The system-dynamic models of information influences in social networks and groups are considered. Their application for purposes of counteraction to information terrorism and extremism is proved. The description in the form of flowcharts is given. Systems of differential equations are presented. Experiments with models using the advanced simulation platform Anylogic were carried out. In a sample of Russian settlements based on cluster analysis found homogeneous typological groups that differ in the average time of transmission of information in social networks. Based on Gibbs ' postulate, the system-dynamic model of information influences among students has been successfully tested. The high consistency of simulation results with empirical data (determination coefficients of at least 90%) is shown. Models allow you to forecast the II and ICA and to play different scenarios of the dynamics of these processes.

Keywords: simulation modeling, information influences, management, social network, topology, typology, cluster analysis.

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. 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.)
3. 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.)
4. 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.)
5. 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.)

6. 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.)
7. 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.)
8. 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.)
9. Alekhnovich S. O., Slizovsky D. E., Ozhiganov E. N. [System-dynamic modeling principles, structure and variables (on the example of Moscow region)]. // RUDN Journal of Political Science. 2009, No 1. – Pp. 22-36. (In Russ.)
10. Forrester J.W. Industrial Dynamics. Waltham (MA): Pegasus Communications, 1961. – 464 p.
11. Forrester J.W. Urban Dynamics. Waltham (MA): Pegasus Communications, 1969. – 285 p.
12. Forrester J.W. World Dynamics. Waltham (MA): Pegasus Communications, 1971. – 144 p.
13. 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.
14. 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.
15. 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.
16. 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.
17. Gusarov A. N., Zhukov D. O., Kosarev A.V. [Description of computer threats spread dynamics in information-computing networks with delay of antiviruses action // Herald of the Bauman Moscow State Technical University. Series Instrument Engineering. 2010. No. 1. – Pp. 112-120. (In Russ.)
18. Gibbs J. Elementary principles of statistical mechanics. NY: Charles Scribner's sons, 1902. – 207 p.