

Перспективой исследований проблемы цифрового разрыва является использование имитационного моделирования в качестве инструментария, позволяющего усовершенствовать существующие подходы к решению проблемы сопротивления персонала. Разработанные на сегодняшний день методологии позволяют моделировать поведение коллектива, в котором итоговое решение о принятии (отторжении) нововведений определяется влиянием многочисленных мнений. Агентный подход позволяет учитывать ментальный фактор при проведении экспериментов с ротацией сотрудников предприятия, локализацией неформальных лидеров, изменением внешних условий с целью оптимизации процесса внедрения инноваций.

Список использованной литературы:

1. Nadler D.A. Beyond the charismatic leader: leadership and organizational change / David A.Nadler, Michael L.Tushman // The training and development sourcebook: second ed.; ed.by G.E.Schneider, R.W.Beatty, L.S.Baird. – NY: HRD Press,1994. – P.278-291.
2. Hofstede G. Dimensionalizing Cultures: The Hofstede Model in Context. Western Washington University [Электронный ресурс]. – Режим доступа: <http://www.wvu.edu/culture/hofstede.htm>

КОНЦЕПТУАЛЬНІ АСПЕКТИ МОДЕЛЮВАННЯ РИЗИКУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

В.В. Вітлінський

м. Київ, ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

Забезпечення життєво важливих інтересів особи, сталою та безпечною розв'язкою регіону, країни є одним із пріоритетних завдань. Проблемам управління економічної безпекою присвячено немало праць, функціонують наукові школи. Українські вчені також зробили значний внесок у цю сферу знань, серед багатьох можна назвати зокрема, В.А. Забродського, М.О. Кизима, Т.С. Клебанову. Значний

доробок у розвиток проблем моделювання й аналізу безпеки і ризику в складних системах має Санкт-Петербурзька наукова школа під керівництвом професорів І.О. Рябініна, Є.Д. Соложенцева. У деяких словниках, зокрема в [1, с. 70] читаємо: «Безпека. Стан. Коли кому-, чому-небудь ніщо не загрожує». Також йдеться про безпеку інформації (даних) – захищеність інформації (даних) від несанкціонованих дій (випадкових чи навмисних). Техногенна безпека – відсутність недопустимого ризику на технологічному об'єкті. У монографії [2] автори слушно стверджують, що «економічна безпека визначається сукупністю чинників, які забезпечують незалежність, стійкість, здатність національної економіки до прогресу, створюють захист життєво важливих інтересів особистості, суспільства, а також економічній і соціальній стабільності суспільства в умовах дестабілізуючого впливу внутрішніх і зовнішніх чинників. Зазначимо, що в [3, с. 558], стійкість, стабільність визначається як здатність економічної системи зберігати певні властивості та характеристики незмінними.

Існує низка означень стійкості, що залежать від специфіки конкретної системи. Всі вони мають біхевіористичний характер і вводяться в процесі аналізу поведінки системи. Згідно з одним із найбільш загальних визначень, лінія поведінки системи називається стійкою стосовно деякої області фазового простору, якщо почавшись всередині цієї області, вона ніколи її не залишає.

Професор Рябінін І.О. стверджує [4, с. 25], що термін «ризик» фігурує як кількісний критерій загрози, іншими словами, небезпека вимірюється ступенем ризику попадання досліджуваної системи в небезпечний стан, який характеризується збитками «великого масштабу».

Долучення до складу аксіоми функціонування економічних систем принципу невизначеності та породженого цим ризику дозволяє адекватніше розглядати складні економічні системи як такі, що саморозвиваються, та на необхідність враховувати й оцінювати їх безпеку.

На нашу думку, **економічна безпека** – це інтегрована системна характеристика, що залежить від надійності

елементів розглядуваної системи, стійкості, допустимого ступеня ризику, керованості параметрів, з метою забезпечення сталого розвитку та захисту життєво важливих економічних інтересів особистості й суспільства, економічної стабільності суб'єктів економічних відносин та економіки країни загалом.

Об'єкти економічної безпеки – це економічні відносини різних рівнів, а економічні інтереси цих рівнів можуть бути як збалансованими, так і ні.

У низці наукових праць, зокрема в [5] зазначається, що загальна теорія сталого та стійкого розвитку на рівні здорового глузду, засвідчує: щоб відчувати себе відносно безпечно окремій людині чи суспільству, необхідно так організувати своє поведіння, щоб мінімізувати зони підвищеного ризику, по можливості «розширити» вузькі місця, моделювати та прогнозувати ризики, створюючи умови для більшої впевненості та безпеки щодо завтрашнього дня (запаси на «чорний день», наявність надійних партнерів, страхування тощо). Тобто зрозуміти загальну концепцію (логіку) формування стійкого та безпечного стану об'єкта в оточуючому середовищі не складає непереборної проблеми. Складніше інакше – реалізувати раціональне поведіння в відповідності з цією логікою. Зазначимо, що важливим (а інколи й вирішальним) моментом у виборі стратегії поведінки об'єкта є ступінь ризику, на який відповідна керуюча система (децидент) внутрішньо згоджується. Якщо йдеться про розвиток соціально-економічної системи, то вибір ступеня ризику – це одночасно й вибір темпів зростання відповідних економічних показників. Можна всі ресурси витратити на безпеку (стабілізацію), мінімізувавши всі можливі на увазі ризики, але водночас законсервуватись від зовнішньої інформації, мінімізувавши розвиток. Альтернативою такій надобережній стратегії є ва-банківська стратегія поведінки.

Зрозуміло, що раціональна соціально-економічна стратегія (політика) має знаходитись десь між двома цими крайніми стратегіями. У багатьох випадках вдається раціонально поєднувати чинники безпеки й інтенсифікації.

Вкладення в стабілізацію та безпеку постійно збільшуються

в умовах ризику несанкціонованого втручання в інформаційні мережі на різних рівнях – від побутового аж до секретної інформації на державному рівні. Науково-технічний прогрес, впровадження інновацій, високий рівень комп'ютерної грамотності населення спонукає швидке нарощування складності виробничо-економічної системи, зростання обсягів інформаційних потоків та запасів, виникнення принципово нової непередбачуваної інформації, що тягне за собою виникнення нових загроз і невідомих до цього ризиків.

Попри те, що на даний час існує низка моделей, методів та інформаційних технологій, які застосовуються в управлінні економічною безпекою, існує нагальна необхідність їх узагальнення та розроблення нових. Йдеться про адекватне застосування методів штучного інтелекту, природних обчислень, гібридного інструментарію.

У межах нелінійної парадигми економічної динаміки доречною є подальша розбудова процедур превентивного оцінювання ступеня ризику, узагальнення та створення нових модифікацій фрактальних та лагово-фрактальних моделей, на підґрунті яких будувати альтернативні траєкторії та сценарії ризиків відповідних економічних систем.

Актуальною є розбудова методологічних положень щодо моделювання, прогнозування, оцінювання та управління інформаційними ризиками в проектуванні, впровадженні корпоративних інформаційних систем з використанням нечітких мереж Петрі з інгібіторними зв'язками. Поширення набуває концепція I^3 -технологій (інтелектуальних, інноваційних, інформаційних) та побудова відповідних моделей для аналізу та управління ризиком в системі економічної безпеки на підґрунті цієї концепції, а також аналізу стійкості в системі інформаційної безпеки та бази так званих ситуаційних моделей.

У наш час, коли у світі поширюється хаос, нестабільність, для безпечного існування й розвитку необхідно також напрацювати певні програми реагування на загрози як внутрішні, так і зовнішні, враховуючи нестабільність природних умов, посилення агресивності як серед індивідуумів, так і між державами; прогнозуючи та

прораховуючи ризики в системі соціально-економічної безпеки на підґрунті застосування математичних методів, моделей та інформаційних технологій.

Список використаних джерел:

1. Великий тлумачний словник сучасної української мови / Уклад. і головн. ред. В.Т. Брусел. – К.: ВТФ «Перун», 2005. – 1728с.
2. Забродский В.А., Кизим Н.А. Собственность, экономическая безопасность и государство. – Харьков: АО «Бизнес Информ», 1997. – 96.с
3. Экономико-математический энциклопедический словарь / гл. ред. В.И. Данилов-Данильян. – М.: Изд. Дом «ИНФА-М», 2003. – 688с.
4. Рябинин И.А. Научная школа «Моделирование и анализ безопасности и риска в сложных системах» и ее смысл / Моделирование и анализ безопасности и риска в сложных системах: Труды Международной Научной Школы МАБР-2004/ГОУ ВПО «СПбГУАП», СПб, 2004. – 649с.
5. Петраков Н.Я. Русская рулетка: экономический эксперимент ценою 150 миллионов жизней. – М.: ОАО «Изд-во «Экономика», 1998. – 286с.

ПРИРОДНІ ОБЧИСЛЕННЯ В МОДЕЛЮВАННІ ЛОГІСТИЧНОГО РИЗИКУ

В.В. Вітлінський, В. І. Скіцько
м. Київ, ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

Перше місце серед глобальних ділових ризиків за версією щорічника Allianz Risk Barometer [1], який кілька років поспіль випускає страхова компанія «Allianz Global Corporate & Specialty» (AGCS) посідає ризик, пов'язаний з порушенням перебігу бізнес-процесів, зокрема, логістичних ланцюгів постачання, тобто логістичний ризик.

Існують різні тлумачення поняття логістичного ризику,