Запобігання та ліквідація надзвичайних ситуацій

УДК 614.8

Р.І. Шевченко

Національний університет цивільного захисту України, Харків

ФОРМУВАННЯ ТЕОРЕТИЧНИХ ОСНОВ ІНФОРМАЦІЙНО-КОМУНІКАТИВНОГО КОМПЕНСУВАННЯ ФУНКЦІОНАЛЬНОЇ КРИТИЧНОСТІ ГІБРИДНИХ СИСТЕМ ВІД ДІЇ ЗОВНІШНЬОГО ВПЛИВУ РІЗНОЇ ПРИРОДИ, В РАМКАХ КОНЦЕПЦІЇ СТВОРЕННЯ МАТЕРІАЛЬНО-ІНФОРМАЦІЙНО-РОЗУМНОЇ СИСТЕМИ МОНІТОРИНГУ НАДЗВИЧАЙНИХ СИТУАЦІЙ

На прикладі системи моніторингу надзвичайних ситуацій природного та техногенного характеру, розроблені теоретичні підходи до моделювання процесів компенсування інформаційно-комунікативної критичності, яка виникає від дії зовнішнього впливу різної природи, в складних гібридних системах.

Ключові слова: *критичність функціонування системи, моніторинг надзвичайних ситуацій, зовнішній вплив.*

Вступ

Постановка проблеми. Відсутність дієвої системи моніторингу надзвичайних ситуацій України, зводить нанівець існуючи організаційні заходи з профілактики небезпечних чинників аварійних стані об'єктів. Підтвердженням цього є щорічна негативна динаміка [1] щодо зростання кількості надзвичайних ситуацій та розміру їх негативних наслідків.

З іншого боку аналіз останніх теоретичних досягнень у сфері формування підходів до створення дієвої системи моніторингу надзвичайних ситуацій [2 – 5], свідчить про відсутність істотних інновацій в цьому напрямку. Все це потребує перегляду, насамперед, концептуальних підходів по побудови системи моніторингу надзвичайних ситуацій, як складної багаторівневої підсистеми єдиної системи запобігання надзвичайним ситуаціям. Остання, в свою чергу повинна формуватися, як матеріально-інформаційно-розумна система. За таких підходів гостро постає проблема розробки сучасного теоретичного апарату з моделювання функціональних станів гібридних систем в складних інформаційно-комунікативних умовах функціонування. Рішенню визначеної проблеми, на прикладі системи моніторингу надзвичайних ситуацій природного та техногенного характеру, і присвячено дане дослідження.

Аналіз останніх досліджень і публікацій. На протязі останніх років були здійснені окремі спроби проаналізувати механізм впливу та розробити окремі рекомендації щодо компенсування нерегламентованого впливу на систему моніторингу надзвичайних ситуацій [6 – 10]. Здебільш природного та техногенного, інколи частково соціального характеру [11 – 13]. Втім основними недоліками попередніх досліджень є відсутність системності у розв'язанні поставленого завдання та здебільш епізодичний та декларативний характер наведених рішень.

Постановка задачі та шляхи її вирішення. У відповідності до запропонованої схеми процесу розробки політики інформаційно-комунікативної безпеки системи моніторингу надзвичайних ситуацій природного та техногенного характеру [14] проведемо інформаційно-комунікативний аналіз компенсуючого впливу на дію зовнішніх чинників різної природи.

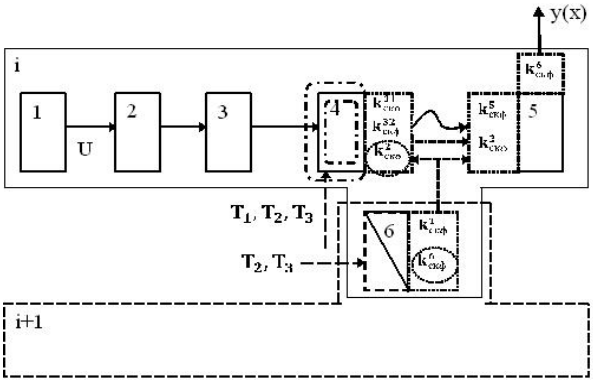

Рис. 1. Схема інформаційно-комунікативного компенсування зовнішнього впливу техногенного характеру на систему моніторингу надзвичайних ситуацій природного та техногенного характеру (де і та і+1 – аналізуєма та впливаюча системи моніторингу відповідно

На рис. 1 позначено: 1 – джерело небезпеки, 2 – підсистема збору та контролю стану джерела небезпеки, 3 – підсистема каналу зв'язку, 4 – інформаційно-комунікативна підсистема, 5 – підсистема прийняття рішення, 6 – підсистема аналізу зовнішнього впливу; U – потік інформації від об'єкту моніторингу; y(x) – управляюче рішення щодо стану об'єкту моніторингу; T_1, T_2, T_3 – інформаційно-комунікативні

критичності викликані факторами зовнішнього техногенного впливу; ▭ – постійно діючи підсистеми, ◹ – тимчасово /або постійно діючи підсистеми відповідно до моделі впливу, ▭ – викривлення інформаційного поля; ▭ – можливість компенсування проявів критичності, ⬭ – можливість часткового компенсування критичності).

На рис. 1 та далі критерії інформаційно-комунікативні критичності системи моніторингу надзвичайних ситуацій такі:

$k^{31}_{\text{скф}}$ – надлишок інформаційного потоку; $k^{32}_{\text{скф}}$ – збитковість інформаційного потоку; $k^{1}_{\text{скф}}$ – залежність інформаційного потоку від розвитку ситуації; $k^{2}_{\text{скф}}$ – часткова недостовірність інформаційного потоку; $k^{5}_{\text{скф}}$ – непередбачуваність ситуації, орієнтація на досвід; $k^{4}_{\text{скф}}$ – високий динаміка змін інформаційного потоку; $k^{322}_{\text{скф}}$ – тимчасова відсутність інформаційного потоку; $k^{\text{фр}}_{\text{скф}}$ – тимчасова відсутність інформації в наслідок фізичного втручання; $k^{6}_{\text{скф}}$ – відсутність дієвості кінцевої цілі; $k^{326}_{\text{скф}}$ – довготривала відсутність інформації; $k^{26}_{\text{скф}}$ – переважно викривлений інформаційний потік.

Зауважимо, що інформаційно-комунікативна система (і) у «базовому» вигляді є досить інерційна та консервативна щодо можливості обробки джерел додаткової інформації, у наслідок обмеженості та консервативності розвитку можливостей тезаурусної складової системи (θ), а від так слід очікувати, від запровадження підсистеми аналізу зовнішнього впливу, двобічного ефекту. Якісна оцінка ефективності компенсування критичностей від зовнішнього впливу техногенного характеру наведена в табл. 1.

Таблиця 1

Якісна оцінка компенсування інформаційно-комунікативних критичностей зовнішнього впливу техногенного характеру

Критичність	«Базовий» рівень критеріїв критичності k^{j}_{b}	Якісна оцінка впливу підсистеми аналізу зовнішнього впливу на рівень критичності (і) системи моніторингу надзвичайних ситуацій $k^{j}_{\text{ÛÛ}}$	
		Позитивний вплив	Негативний вплив
T_1	k^{32}_{b}	$k^{32}_{\text{ÛÛ}} \lll k^{32}_{b}$	$k^{31}_{\text{ÛÛ}} \neq 0;\ k^{5}_{\text{ÛÛ}} \neq 0$
T_1, T_2	k^{31}_{b}		$k^{31}_{\text{ÛÛ}} \gg k^{31}_{b}; k^{5}_{\text{ÛÛ}} \neq 0$
T_1, T_2	k^{1}_{b}	$k^{1}_{\text{ÛÛ}} \lll k^{1}_{b}$	$k^{32}_{\text{ÛÛ}} \neq 0 \text{ if } t \neq t^{\text{inc}}_{\text{eaT}}$ $k^{31}_{\text{ÛÛ}} \neq 0 \text{ if } t \neq t^{\text{off}}_{\text{eaT}}$
T_2	k^{5}_{b}	$k^{5}_{\text{ÛÛ}} < k^{5}_{b}$	
T_3	k^{2}_{b}	$k^{2}_{\text{ÛÛ}} \lll k^{2}_{b}$	
T_3	k^{6}_{b}	$k^{6}_{\text{ÛÛ}} \lll k^{6}_{b}$	

Аналогічну процедуру застосуємо до аналізу зовнішнього впливу природного характеру рис. 2 та табл. 2. Зазначимо, що для системи моніторингу (і) надзвичайних ситуацій, яка знаходиться під зовнішнім впливом природного характеру можливі 2 критичних стани, а саме: k^{322}_{b} – тимчасова (Δt_{322}) відсутність інформації про стан об'єкту моніторингу, часткове компенсування якої можливе лише на рівні комунікативно-компенсуючих фільтрів тезаурусної складової із застосування експертної системи та прогнозування поведінки об'єктів моніторингу виходячи з наявних рішень у базі даних, при ($\Delta t_{322} \to 0$) та відсутності безпосереднього впливу на об'єкт моніторингу зовнішнього впливу природного характеру, можна висловити припущення про стабільний стан об'єкту та зневажати на наявну критичність; $k^{\text{фр}}_{b}$ – критичність викликана фізичним впливом на підсистеми моніторингу, та призводить до часткової (k^{32}_{b}) або повної відсутності інформації (k^{322}_{b}) на час дії впливу, частково компенсується підсистемою аналізу впливу, потребує передбачення системи фізичного та інформаційно-комунікативного захисту від зовнішніх впливів.

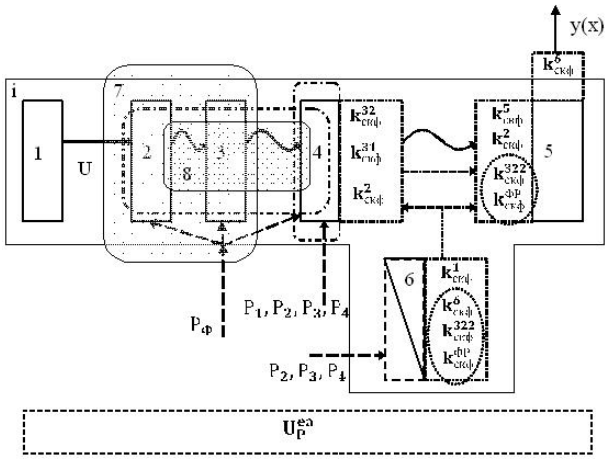

Рис. 2. Схема інформаційно-комунікативного компенсування зовнішнього впливу природного характеру на систему моніторингу надзвичайних ситуацій природного та техногенного характеру (де і та U^{ea}_P – аналізуєма система моніторингу та зовнішній вплив природного характеру відповідно; P_1, P_2, P_3, P_4 – інформаційно-комунікативні критичності викликані факторами зовнішнього техногенного впливу; P_ϕ – фізична критичність викликана фактором зовнішнього впливу; 7 та 8 – підсистеми фізичного захисту та інформаційно-комунікативного захисту інформації відповідно)

Як зазначалось раніше зовнішній вплив техногенного та природного характеру на систему моніторингу слід розглядати як додаткове критичне навантаження, для подолання якого система має функціональні та технічні можливості, за умов формування чіткої організаційної та інформаційно-комунікативної структури, удосконалення та узгодження методологічної та технічної бази системи. Зовсім інша річ нерегламентований вплив факторів соціального характеру. Компенсування яких можливо лише частково та носить складний багаторівневий характер. Моделювання відповідного процесу представлено на рис. 3.

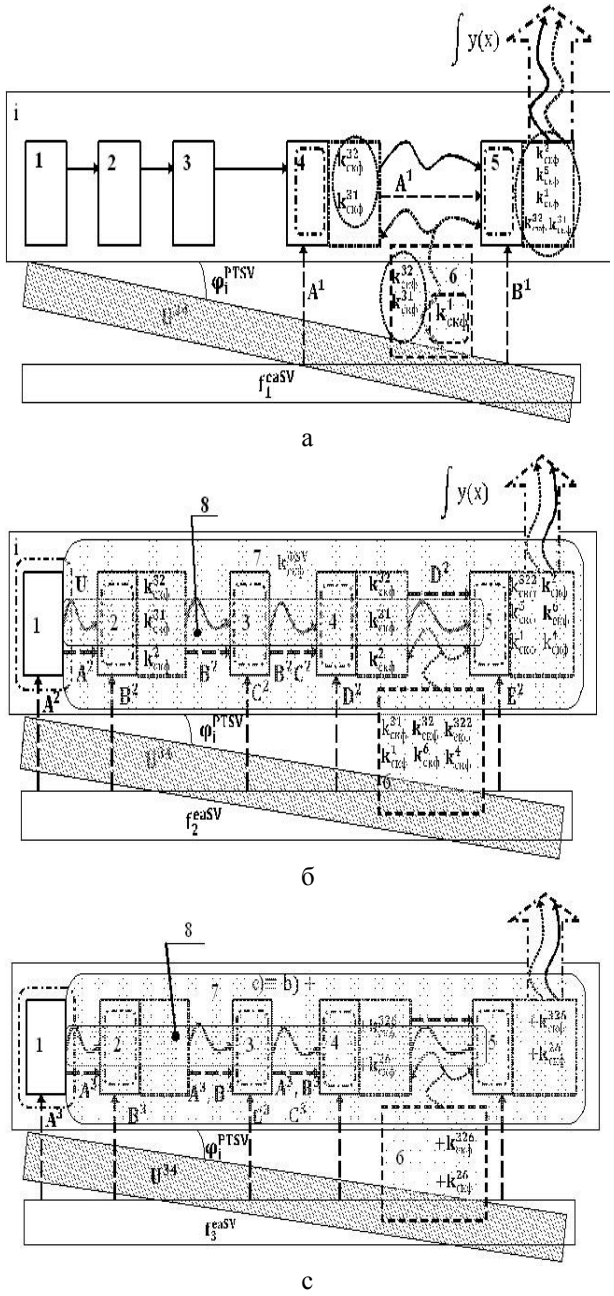

Рис. 3. Стала схема інформаційно-комунікативного компенсування нерегламентованого впливу соціального характеру на систему моніторингу надзвичайних ситуацій природного та техногенного характеру, де а – вплив фактору f_1^{eaSV} – соціальна напруга; б – вплив фактору f_2^{eaSV} – тероризм; с – вплив фактору f_3^{eaSV} – воєнні дії

На рис. 3: U^{34} – система моніторингу надзвичайних ситуацій та система моніторингу соціальної напруги відповідно; 1 – джерело небезпеки, 2 – підсистема збору та контролю стану джерела небезпеки, 3 – підсистема каналу зв'язку, 4 – інформаційно-комунікативна підсистема, 5 – підсистема прийняття рішення, 6 – нерегламентована (неіснуюча) підсистема аналізу зовнішнього впливу, 7 та 8 – підсистеми фізичного захисту та інформаційно-комунікативного захисту інформації відповідно; U – потік інформації від об'єкту моніторингу; $\int y(x)$ – управляюче рішення інтегрального характеру щодо стану об'єкту моніторингу; A^1, B^1 – інформаційно-комунікативні критичності викликані f_1^{eaSV} фактором зовнішнього соціального впливу; A^2, B^2, C^2, D^2, E^2 – інформаційно-комунікативні критичності викликані f_2^{eaSV} фактором зовнішнього соціального впливу; A^3, B^3, C^3, D^3, E^3 – інформаційно-комунікативні критичності викликані f_3^{eaSV} фактором зовнішнього соціального впливу φ_i^{PTSV} – кут неузгодженості інформаційних потоків; ▭ – постійно діючи підсистеми; ▭ – нерегламентована /неіснуюча підсистема/ або неможливість компенсування критичності; ▭ – викривлення інформаційного поля; ▭ – можливість компенсування проявів критичності; ▭ – можливість часткового компенсування критичності).

Результати аналізу компенсування для нерегламентованого впливу соціального характеру, за визначеною раніше для природного та техногенного зовнішніх впливів методологією наведено у табл. 3.

Таблиця 2

Якісна оцінка компенсування інформаційно-комунікативних критичностей зовнішнього впливу природного характеру

Критичність	«Базовий» рівень критеріїв критичності k_b^j	Якісна оцінка впливу підсистеми аналізу зовнішнього впливу на рівень критичності (i) системи моніторингу надзвичайних ситуацій $k_{\overline{UU}}^j$	
		Позитивний вплив	Негативний вплив
P_1	k_b^{32}	$k_{\overline{UU}}^{32} \lll k_b^{32}$	$k_{\overline{UU}}^{31} \neq 0;\ k_{\overline{UU}}^{5} \neq 0$
P_1, P_3, P_4	k_b^{31}		$k_{\overline{UU}}^{31} \gg k_b^{31};\ k_{\overline{UU}}^{5} \neq 0$
P_1, P_3	k_b^{1}	$k_{\overline{UU}}^{1} \lll k_b^{1}$	$k_{\overline{UU}}^{32} \neq 0$ if $t \neq t_{eaP}^{inc}$ $k_{\overline{UU}}^{31} \neq 0$ if $t \neq t_{eaP}^{off}$
P_3	k_b^{5}	$k_{\overline{UU}}^{5} < k_b^{5}$	
P_4	k_b^{2}	(рівень M) $k_{\overline{UU}}^{2} < k_b^{2}$ (рівень R) $k_{\overline{UU}}^{2} \ll k_b^{2}$	$k_{\overline{UU}}^{31} \gg k_b^{31};\ k_{\overline{UU}}^{5M} \neq 0$ $k_{\overline{UU}}^{31} \ggg k_b^{31};\ k_{\overline{UU}}^{5R} > k_{\overline{UU}}^{5M}$
P_4	k_b^{6}	$k_{\overline{UU}}^{6} \lll k_b^{6}$	
P_2	k_b^{322}	$k_{\overline{UU}}^{322} < k_b^{322}$	$k_{\overline{UU}}^{2} \neq 0;\ k_{\overline{UU}}^{5} \neq 0$
P_Φ	$k_b^{\Phi P}$	$k_{\overline{UU}}^{\Phi P} < k_b^{\Phi P}$	$k_{\overline{UU}}^{2} \neq 0;\ k_{\overline{UU}}^{5} \neq 0$

Зазначимо, що це можливо у разі наступних припущень (взаємозв'язок систем моніторингу U^6 існує та принаймні для частини об'єктів моніторингу регламентований інформаційно-комунікативний обмін):

$$\varphi_i^{PTSV} \to 0 \ \text{ та } \ U^{34} \equiv U^6 \neq 0\,. \qquad (1)$$

У разі невиконання умови (1) прогнозуємий стан критичностей системи моніторингу надзвичайних ситуацій з часом зростає значно перевищуючи базовий (на час початку впливу нерегламентованих факторів соціального характеру), а саме виконуються рівняння:

$$k_{\overline{UU}}^{i} > k_b^{i} \quad \text{if} \quad k_b^{i} \in (SV_1 \vee SV_2)\,; \qquad (2)$$

$$k_{\overline{UU}}^{i} >> k_b^{i} \quad \text{if} \quad k_b^{i} \in (SV_3)\,; \qquad (3)$$

$$k_{\overline{UU}}^{i} >>> k_b^{i} \quad \text{if} \quad k_b^{i} \in (SV_4 \vee SV_5)\,. \qquad (4)$$

Враховуючи розбіг природи критичностей (SV) та відповідних можливостей компенсування системи моніторингу надзвичайних ситуацій у разі виникнен-

ня кризових станів (326, 26, 322) відтворити дійсну картину стану об'єктів моніторингу за допомоги компенсуючого потоку U^{34} не можливо, а від так необхідно передбачити ефективні заходи превентивного характеру через вплив систем 7 та 8.

Таблиця 3

Якісна оцінка можливостей компенсування інформаційно-комунікативних критичностей зовнішнього впливу соціального характеру за рахунок інформаційного потоку U^{34}

Рівень впливу	Критичність	«Базовий» рівень критеріїв критичності k_b^j	Якісна оцінка впливу інформаційного потоку системи моніторингу соціальної напруги на стан критичності (і) системи моніторингу надзвичайних ситуацій $k_{\widetilde{U}U}^j$	
			Позитивний вплив	Негативний вплив
A^1 B^1	SV_1	k_b^{32} k_b^{31} k_b^2 k_b^5 k_b^1	$k_{\widetilde{U}U}^{32} \lll k_b^{32}$ $k_{\widetilde{U}U}^{2} \ll k_b^{2}$ $k_{\widetilde{U}U}^{5} \ll k_b^{5}$ $k_{\widetilde{U}U}^{5} \ll k_b^{5}$	$k_{\widetilde{U}U}^{31} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{31} \gg k_b^{31};k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$
A^2 B^2 C^2 A^3 B^3 C^3	SV_1 SV_2 SV_3	k_b^{32} k_b^{31} k_b^2 k_b^1 k_b^{322} $k_b^{\phi SV}$	$k_{\widetilde{U}U}^{32} \lll k_b^{32}$ $k_{\widetilde{U}U}^{2} \ll k_b^{2}$ $k_{\widetilde{U}U}^{1} \ll k_b^{1}$ $k_{\widetilde{U}U}^{322} < k_b^{322}$ $k_{\widetilde{U}U}^{\phi SV} < k_b^{\phi SV}$	$k_{\widetilde{U}U}^{31} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{31} \gg k_b^{31};k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{2} \gg k_b^{2}$ $k_{\widetilde{U}U}^{2} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$
D^2 E^2	SV_2 SV_3 SV_5	k_b^{32} k_b^{31} k_b^2 k_b^1 k_b^{322} k_b^4 k_b^5 k_b^6	$k_{\widetilde{U}U}^{32} \lll k_b^{32}$ $k_{\widetilde{U}U}^{2} \ll k_b^{2}$ $k_{\widetilde{U}U}^{1} \ll k_b^{1}$ $k_{\widetilde{U}U}^{322} < k_b^{322}$ $k_{\widetilde{U}U}^{5} < k_b^{5}$ $k_{\widetilde{U}U}^{6} < k_b^{6}$	$k_{\widetilde{U}U}^{31} > k_b^{31}$ $k_{\widetilde{U}U}^{31} \gg k_b^{31};k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{31} \neq 0$ $k_{\widetilde{U}U}^{2} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{4} \equiv k_b^{4}$ $k_{\widetilde{U}U}^{31} > k_b^{31}$
D^3 E^3	SV_2 SV_3 SV_5 $+SV_4$	$k_b^{32},k_b^{31},k_b^2,$ $k_b^1,k_b^{322},k_b^4,$ k_b^5,k_b^6 $+k_b^{326}$ $+k_b^{26}$	$k_{\widetilde{U}U}^{326} < k_b^{326}$ $k_{\widetilde{U}U}^{26} < k_b^{26}$	$k_{\widetilde{U}U}^{2} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$ $k_{\widetilde{U}U}^{2} \neq 0;\ k_{\widetilde{U}U}^{5} \neq 0$

Досягнення ефективності можливе лише за вимоги комплексного підходу до забезпечення інформаційно-комунікативної безпеки через низку заходів:

$$U_e^{PTSV} = \int (U^{34}, F_7(U), F_8(U)), \qquad (5)$$

де $F_7(U), F_8(U)$ – комплекс заходів направлений на забезпечення інформаційно-комунікативної безпеки в рамках застосування систем 7 та 8 (рис. 3).

Розглянемо динаміку зміни критичності системи моніторингу надзвичайних ситуацій викликану зовнішнім впливом природного або техногенного характеру та прогнозуєму дієвість управляючого рішення щодо об'єкту моніторингу.

Аналіз наявних часових періодів розвитку критичності системи моніторингу надзвичайних ситуацій дозволив поділити відповідний процес на декілька принципово різних часових зон, а саме:

період сталого функціонування

I часова зона $t \in [0...t_{TP}^{inc}]$ – період сталого функціонування та можливої «скритої критичності» від

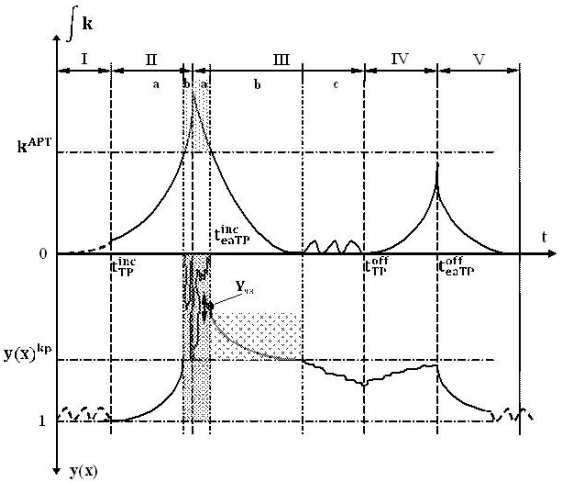

Рис. 4. Динаміка зміни інтегрального показнику критичності $\int k$ системи моніторингу надзвичайних ситуацій від зовнішнього впливу природного та техногенного характеру та зміна прогнозуємої ефективності впливу управляючого рішення y(x) на об'єкт моніторингу

На рис. 4: $\int k$ – показник (інтегральної) критичності системи моніторингу надзвичайних ситуацій, y(x) – дієвість управляючого рішення щодо стану безпеки об'єкту моніторингу, яка знаходиться в межах [0…1]; k^{APT} – межа інформаційно-комунікативної критичності; $y(x)^{kp}$ – межа стабільності контролю (управління) за об'єктом моніторингу; I, II, III, IV, V, a, b, c – часові зони та підзони розвитку процесу критичності в системі моніторингу в межах часового інтервалу t; t_{TP}^{inc}, t_{TP}^{off} – час початку та кінця зовнішнього впливу техногенного (T) або природного (P) характеру; t_{eaTP}^{inc}, t_{eaTP}^{off} – час початку та кінця дії підсистеми оцінки зовнішнього впливу та компенсування викликаної цим впливом критичності; $Y_{чз}$ – рівень дієвості управління на початку відновлення контролю над об'єктом моніторингу у процесі компенсування критичності).

дії зовнішнього впливу, яка характеризується досить стабільною (незначно флуктуючою) дієвістю контролю за об'єктом моніторингу, критичність системи моніторингу постійно корегується за рахунок детермінованого надходження інформації планових та позапланових перевірок об'єкту контролю;

період критичного функціонування

II часова зона $t \in [t_{TP}^{inc}...t_{eaTP}^{inc})$ – період різкого зростання критичності за відсутності компенсування, що характеризується двома підзонами:

IIa – зростання критичності системи до межі інформаційно-комунікативної критичності системи, що визначається з погляду фізіологічних можливостей людини екстремальної тезаурусної обробки та розуміння інформації [28] та на короткий проміжок часу

$$U_{kp}^{\theta} = (10^2...10)U_{ct}^{\theta} \leq 70 бит/с, \qquad (6)$$

де $U_{ст}^{\theta}$ – межі інформаційного потоку сталого процесу функціонування, який характеризується «комфортним режимом» [21] тезаурусної обробки інформації та прийняття рішень та дорівнює (0,1 – 5,5 бит/с), цей період характеризується падінням дієвості контролю за об'єктом моніторингу до межі стабільності;

IIb – зростання критичності систем понад інформаційно-комунікативні можливості системи, та входження в зону функціональної нестабільності системи моніторингу, а від так відсутність адекватної оцінки управляючого впливу на об'єкт моніторингу, дієвість дій управляючого інформаційного потоку можлива в межах [0,1] та непередбачувана.

III часова зона $t \in [t_{eaTP}^{inc} ... t_{TP}^{off})$ – період функціонування системи в режимі інформаційно-комунікативного компенсування дії зовнішнього впливу, характеризується трьома підзонами.

IIIa – зменшення критичності до межі інформаційно-комунікативних можливостей системи. Стан системи моніторингу надзвичайних ситуацій можна вважати аналогічним стану підзони IIb з тією різницею, що розпочато процес компенсування інформаційно-комунікативної критичності.

Підзони IIb та IIIa – формують умовну «чорну» зону непрозорості управління, яка характеризується відсутністю реальної картини щодо стану об'єкту моніторингу та непередбаченістю реакції на управлінський вплив, а саме люба дія може спровокувати початок розвитку надзвичайної ситуацій /аварійного режиму на об'єкті моніторингу.

IIIb – зменшення критичності в межах інформаційно-комунікативних можливостей системи моніторингу, що характеризується зростаючим відновленням контролю над об'єктом моніторингу з боку управлінського впливу до межі стабільного контролю (умовно «сіра» зона – ефективність управління обмежена). Характерним для цього часового періоду є наявність точки виходу системи з неконтрольованої зони управлінського впливу $Y_{чз}$ значення якої непередбачуване та характеризується рівнянням:

$$\text{if} \int k = k^{APT} \Rightarrow Y_{чз} \to 0 \text{ if } t \in (IIb + IIIa). \quad (7)$$

Зона обмеженої надійності, управлінський вплив може погіршити безпечний стан об'єкту моніторингу.

IIIc – флуктація критичності в межах інформаційно-комунікативних можливостей системи моніторингу надзвичайних ситуацій. Характеризується флуктаціями дієвості управлінського впливу за умов загальної тенденції до зростання за межами критичності управління.

IV – часова зона $t \in [t_{TP}^{off} ... t_{eaTP}^{off})$ – період функціонування системи в режимі інформаційно-комунікативного компенсування без дії зовнішнього впливу в наслідок інерційності системи та відсутності чітких функціональних взаємозв'язків. Характеризується зростанням критичності в межах інформаційно-комунікативних можливостей системи та флуктаціями дієвості управлінського впливу за умов загальної тенденції зменшення до межі критичності управління (період небезпечної пост критичності).

V – часова зона $t \in [t_{eaTP}^{off} ... \infty)$ – період зменшення критичності та стале функціонування системи. Характеризується зростанням ефективності управлінського впливу на об'єкт моніторингу та стабілізацією в межах флуктаційних коливань.

Застосування запропонованої методології аналізу інформаційно-комунікативної критичності системи моніторингу надзвичайних ситуацій дозволяє отримати картину покомпонентного внеску критичностей до інтегрального показнику та припустити їх часову залежність (де детермінований крок (Δt) – проміжок часу в межах якого можлива обробка інформацій при екстремальному її надходженні, а від так можливості функціонування системи на межі стійкості) (табл. 4). Функція, яка характеризує характер змін критичності від часу з погляду на аналіз існуючих робіт [15 – 21] може приймати лінійний, степеневий, експоненціальний вигляд або, як у випадку з (k^{322}), фактично імпульсний характер.

Таблиця 4

Оцінка покомпонентного внеску в розвиток і нтегральної критичності системи моніторингу надзвичайних ситуацій по часовим зонам

Природа впливу	k^{ijq}	Внесок до інтегрального показнику критичності $\pm C^{ijq} f(\Delta t^n)$									
		$\pm C^{ijq}$					n				
		Часові зони зміни критичності системи									
		I	II	III	IV	V	I	II	III	IV	V
ТР	k^1	-	C^1	$1-1/C^1$	C^1	-	-	1	3	1	-
	k^2	C^2	C^2	$1-1/C^2$	C^2	-	2	2	2	2	-
	k^{31}	-	C^{31}	C^{31}; $1-1/C^{31}$	C^{31}	-	-	1	1;3	1	-
	k^{32}	-	C^{32}	$1-1/C^{32}$	C^{32}	-	-	1	3	1	
	k^5	-	C^5	$1-1/C^5$	C^5	$1-1/C^5$	-	2	2	2	2
	k^6	-	C^6	$1-1/C^6$	C^6	$1-1/C^6$	-	3	1	3	1
Р	k^{322}	-	C^{322}	$1-1/C^{322}$	-	-	-	4	1	-	-

Висновки

В роботі вперше, на прикладі системи моніторингу надзвичайних ситуацій природного та техногенного характеру, розроблені теоретичні підходи до моделювання процесів компенсування інформаційно-комунікативної критичності в складних гібридних системах від зовнішнього впливу різної природи. Розглянуті позитивні та негативні тенденції стійкості функціонування системи моніторингу та ефективності управління об'єктом контролю в різних режимах компенсування. Наведені окремі рекомендації щодо шляхів створення сучасної дієвої системи моніторингу надзвичайних ситуацій України, що відповідає інноваційним тенденціям сьогодення в рамках концепції єдиної матеріально-інформаційно-розумної системи запобігання надзвичайним ситуаціям.

Список літератури

1. Національна доповідь про стан техногенної та природної безпеки в Україні у 2014 році [Електронний

ресурс]. – Режим доступу: www.mns.gov.ua/content/annual_report_2014.html

2. Національна доповідь про стан техногенної та природної безпеки в Україні у 2013 році [Електронний ресурс]. – Режим доступу: www.mns.gov.ua/content/annual_report_2013.html.

3. Абрамов Ю.А. Основные требования к созданию единой системы мониторинга чрезвычайных ситуаций / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Системи обробки інформації. – Х.: ХУПС, 2005. – Вып. 6 (46). – С. 203-207.

4. Абрамов Ю.А. Взаимосвязь инициирующих и поражающих факторов чрезвычайных ситуаций природного характера на территории Украины / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Проблеми надзвичайних ситуацій. – Х.: УЦЗУ 2007. – Вип. 5. – С. 8-17.

5. Макиев Ю.Д. Аннотация на монографию «Современные системы мониторинга и прогнозирования чрезвычайных ситуаций»: Стратегия гражданской защиты: проблемы и исследования / Ю.Д. Макиев. – 2014. – Том 4, № 1(6). – С. 85-90.

6. Журавлёв Д.А. Реализация мониторинга в системе спутниковой связи в условиях внешнего воздействия/ Д.А. Журавлёв // Scientific researches and their practical application. Modern state and ways of development. 2012 [Електронний ресурс]. – Режим доступу: .http://www.sworld.com.ua/index.php/ru/conference/the-content-ofconferences/archives-of-individual-conferences/oct-2012

7. Шевченко Р.І. Визначення показників небезпеки факторів зовнішнього впливу на ПНО / Р.І. Шевченко, Д.В. Тарадуда // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: мат-ли XIX міжнар. наук.-пр. конф. – Х.: НТУ «ХПІ», 2011. – С. 240.

8. Природні та техногенні загрози, оцінювання небезпек / В.А. Андронов, А.С. Рогозін, О.М. Соболь та інші: навч. посіб. – Х.: НУЦЗУ, 2011. – 264 с.

9. Кластерный анализ территории Украины по основным показателям повседневного функционирования и проявления техногенной опасности / В.В. Тютюник, Н.В. Бондарев, Р.І. Шевченко та інші // Геоінформатика. – К.: Інститут геологічних наук НАН України, 2014. – № 4(52). – С. 63-72.

10. Розробка науково-технічних основ створення системи моніторингу за зонами взаємного ризику від стаціонарних і рухомих потенційно небезпечних об'єктів / В.В. Тютюник, О.М. Соболь, Р.І. Шевченко та інші // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 3(39). – С. 150-156.

11. Коврегін В.В. Формування методологічних підходів до визначення коефіцієнтів безпеки основних елементів аміачної холодильної установки за критерієм «вплив суб'єкта» / В.В. Коврегін, Д.В. Тарадуда, Р.І. Шевченко // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2011. – Вип. 1 (27). – С. 233-236.

12. Тарадуда Д.В. Застосування багатомірної імітаційної моделі стану безпеки об'єкта як предмета управління промисловою безпекою потенційно небезпечних об'єктів / Д.В. Тарадуда, Р.І. Шевченко, Ю.В. Клімчук // Проблеми надзвичайних ситуацій. – Зб. наук. пр. – Х.: НУЦЗУ 2012. – Вип. 15. – С. 166-178.

13. Шевченко Р.І. Оцінка ефективності інтегрованої системи безпеки функціонування підприємств нафтопереробної промисловості / Р.І. Шевченко, П.В. Одарюк, В.В. Тютюник // Проблемы пожарной безопасности. – Сб. науч. тр. – Х.: АГЗУ, 2005. – Вып. 18. – С. 185-191.

14. Шевченко Р.І. Формування політики інформаційно-комунікативної безпеки системи моніторингу надзвичайних ситуацій природного та техногенного характеру / Р.І. Шевченко // Мат-ли 17 Всеукраїнської НПК рятувальників «Сучасний стан цивільного захисту України: Перспективи та шляхи до європейського простору». – К.: ІДУЦЗ, 2015. – С. 438-441.

15. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2007. – 225 с.

16.Лалушкин Ю.П. Проблемы безопасности предоставления информации в системе поддержки принятия решения / Ю.П. Лалушкин, А.В. Бацула // Специальная техника и информационная безопасность. – 1997. – С. 368-369.

17.Фисун А.П. Моделирование и оценка угроз информационной безопасности / А.П. Фисун // Специальная техника и информационная безопасность. – 1997. – С. 382-384.

18. Бочков М.В. Концептуальная модель системы мониторинга безопасности информационного процесса в АСУ / М.В. Бочков, А.В. Королев // Специальная техника и информационная безопасность. – 1997. – С. 387-389.

19. Маслова Н.А. Принципы адаптации в защите корпоративних систем / Н.А. Маслова, В.В. Шамаев // Штучний інтелект. – 2010. – № 4. – С. 421-429.

20. Гришина Н.В. Организация комплексной системы защиты информации / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

21. Меленец А.В. Архитектура интеграции облаков распределенной системы хранения, оперативного обновления и предоставления данных о потенциально опасных объектах на основе технологии Cloud Computing / А.В. Меленец // Радіоелектронні і комп'ютерні системи. – 2012. – № 7 (59). – С. 54-59.

Надійшла до редколегії 18.11.2015

Рецензент: д-р техн. наук, проф. М.І. Адаменко, Харківський національний університет ім. В.Н. Каразіна, Харків.

ФОРМИРОВАНИЕ ТЕОРЕТИЧЕСКИХ ОСНОВ ИНФОРМАЦИОННО-КОМУНИКАТИВНОЙ КОМПЕНСАЦИИ ФУНКЦИОНАЛЬНОЙ КРИТИЧНОСТИ ГИБРИДНЫХ СИСТЕМ ОТ ВНЕШНЕГО ВОЗДЕЙСТВИЯ РАЗЛИЧНОГО ХАРАКТЕРА ВОЗНИКНОВЕНИЯ, В РАМКАХ КОНЦЕПЦИИ СОЗДАНИЯ МАТЕРИАЛЬНО-ИНФОРМАЦИОННО-РАЗУМНОЙ СИСТЕМЫ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Р.И. Шевченко

В работе, на примере системы мониторинга чрезвычайных ситуаций природного и техногенного характера, разработаны теоретические подходы к моделированию процессов компенсации информационно-коммуникативной критичности, которая возникает от внешнего воздействия различной природы, в сложных гибридных системах.

Ключевые слова: *критичность функционирования системы, мониторинг чрезвычайных ситуаций, внешнее воздействие.*

FORMATION THEORETICAL FOUNDATIONS OF INFORMATION AND COMMUNICATION OFFSET FUNCTIONAL CRITICAL HYBRID SYSTEMS FROM OUTSIDE INFLUENCE OF DIFFERENT NATURE, IN CREATING CONCEPT MATERIAL INFORMATION SYSTEM MONITORING OF REASONABLE EMERGENCIES

R.I. Shevchenko

In this paper, the example system monitoring of natural and man-made, developed theoretical approaches to modeling processes compensation information and communication criticality arising from outside influence of different nature, in a complex hybrid systems.

Keywords: *criticality of the system, monitoring of emergencies, external influence.*