

Міністерство України з питань надзвичайних ситуацій
та у справах захисту населення від наслідків Чорнобильської катастрофи

Університет цивільного захисту України

Тютюнник В.В., Шевченко Р.І.

СИСТЕМА ІНТЕГРАЛЬНОЇ БЕЗПЕКИ ОБ'ЄКТІВ ЗАХИСТУ

Харків 2010

Тютюник В.В., Шевченко Р.І. Система інтегральної безпеки об'єктів захисту. – Харків: УЦЗУ, 2009. – 78 с.

Видання призначено для фахівців у галузі розробки та побудови систем безпеки об'єктів, працівників МНС України, курсантів, студентів та слухачів вищих закладів освіти III та IV рівнів акредитації, які навчаються за спеціальністю „Цивільний захист” (затверджено до друку Вченою радою УЦЗУ, протокол № 5 від 24.12.2009 року)

Рецензенти:

доктор технічних наук О.М. Соболев – начальник кафедри „Управління та організації діяльності у сфері цивільного захисту” Університету цивільного захисту України;

кандидат технічних наук, доцент І.О. Громико – професор кафедри „Захисту інформації” Харківського національного університету внутрішніх справ

Монографія „Система інтегральної безпеки об'єктів захисту” увібрала в себе останні теоретичні та практичні наробки в галузі формування та побудови систем інтегральної безпеки від об'єктового до регіонального рівнів. Визначені концепція, основні вимоги та принципи побудови систем інтегральної безпеки, останні проілюстровано практичними прикладами для найбільш поширених складових системи інтегральної безпеки.

© Тютюник В.В.,

Шевченко Р.І.

© УЦЗУ, 2009

ВСТУП

Територія України, як об'єкт життєдіяльності, є складною системою з територіально-часовим розподілом параметрів з необхідністю забезпечення безпеки її функціонування в умовах дії небезпечних чинників надзвичайних ситуацій (НС).

Незважаючи на заходи, направлені на забезпечення безпеки, кількість НС на території України не зменшується. Як бачимо, представлений розподіл (рис. В.1, рис. В.2) [2 – 8] досить переконливо доводить динаміку стабільного погіршення стану безпеки регіонів України та свідчить про недосконалість державної системи безпеки і відповідно малу ефективність регламентованих заходів.

Щороку в Україні відбувається понад 300 надзвичайних ситуацій природного, техногенного і соціального характеру – рис. В.3. При цьому спостерігається стійкий зв'язок між видами НС. Так, наприклад, надзвичайні ситуації природного характеру досить часто призводять до виникнення надзвичайних ситуацій техногенного та соціального характеру.

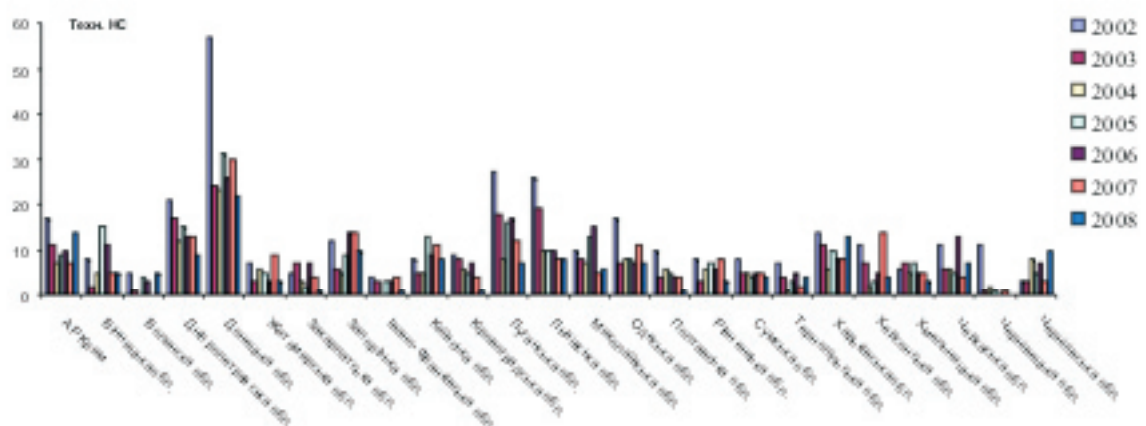


Рис. В.1 – Розподіл по території України надзвичайних ситуацій техногенного характеру у період 2002-2008 рр.

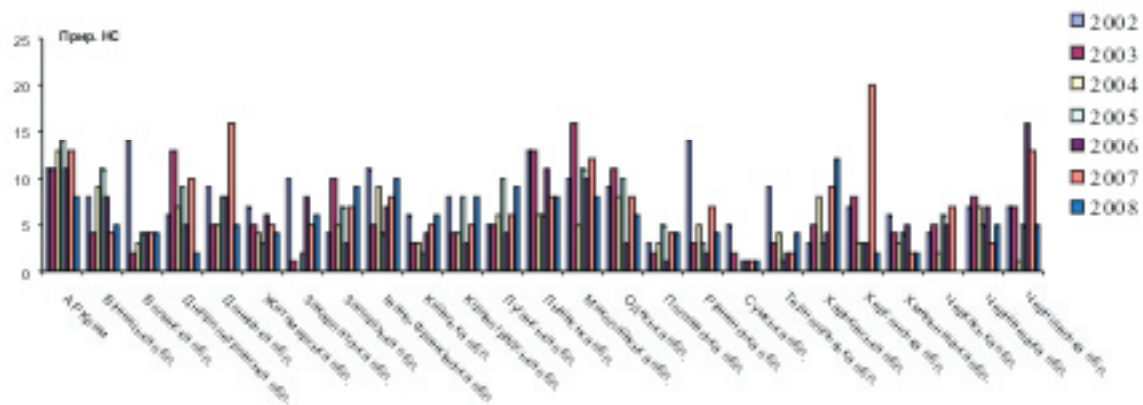


Рис. В.2 – Розподіл по території України надзвичайних ситуацій природного характеру у період 2002-2008 рр.

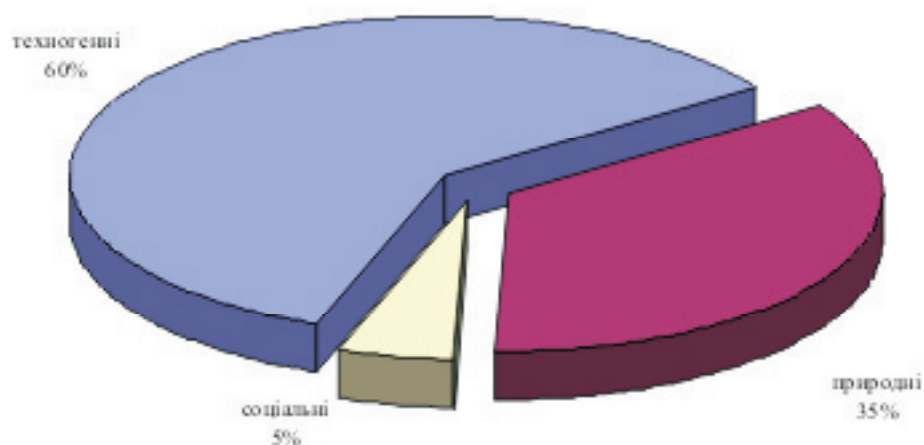


Рис. В.3 – Процентне співвідношення кількості НС, що виникли на Україні (2000 – 2008 рр.)

Наслідком розуміння даного факту є необхідності комплексного підходу до вирішення проблеми забезпечення безпеки функціонування об'єктів на території України, як природно-техногенно-соціальної (ПТС) системи, аналіз і оцінка стану безпеки яких переконливо доводить, що в силу цілого ряду соціальних, економічних і демографічних факторів загрози в ПТС системах у найближчій час матимуть стійку динаміку росту [9 – 11]. Ці загрози у свою чергу здатні створювати та посилювати ряд нових загроз. Вони характеризуються винятково високими градієнтами вторичних факторів, які вражають населення і навколишнє

середовище в моменти їх виникнення і розвитку, тому під час розгляду ПТС систем особливо важливим є визначення комплексного ризику, що, в свою чергу, дає змогу оцінити вплив на стан безпеки різномірних часових і просторових факторів, визначити їх якісні та кількісні характеристики.

Сучасне суспільство, прагнучи установити своє панування над природою, зіштовхнулося із ситуацією, коли функціонування штучно створеної «другої природи» – техносфери все частіше набуває критичного характеру розвитку, обертається катастрофічними наслідками [12 – 15]. Конфлікт, між людською діяльністю і навколишнім середовищем з її пристосуванням до суспільних потреб все частіше призводить до природних, техногенних, соціальних катастроф (рис. В.4).

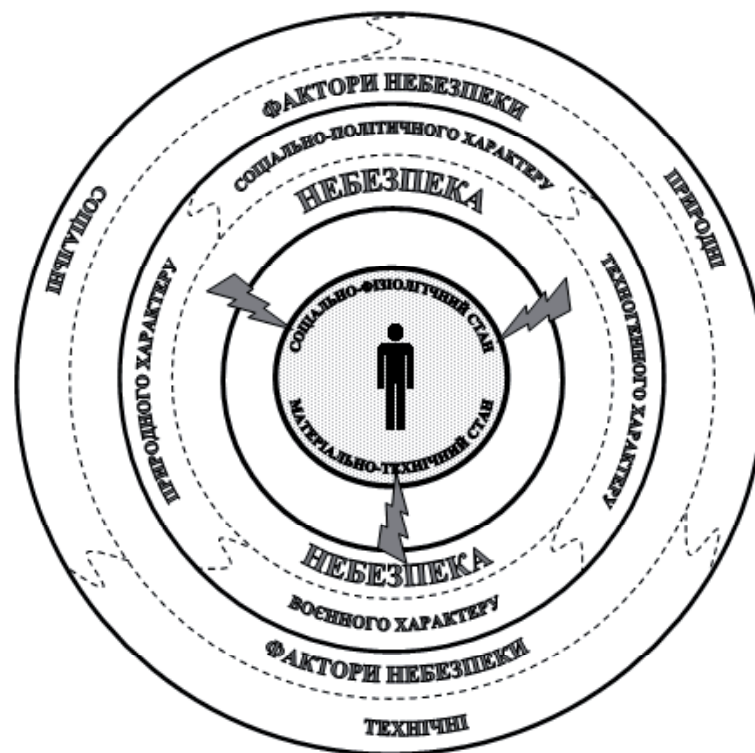


Рис. В.4 – Концепція безпеки соціуму в умовах надзвичайних ситуаціях

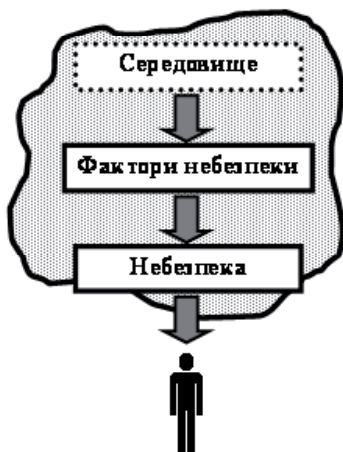
Людина, суспільство, технологічні процеси, потрапляючи в екстремальний режим функціонування [16, 17], мають декілька можливих шляхів зміни: від розпаду до стійкого розвитку [18]. Катастрофи призводять до порушення нормального економічного, соціального, політичного, духовного розвитку суспільства

або його частини, супроводжуються великими людськими і матеріальними втратами [19 – 21].

Природні катастрофи є наслідком дії стихійних сил природи. Людство поки не в змозі їх цілком запобігти. Але своєю діяльністю, наприклад, досліджуючи їх, воно може мінімізувати втрати, і навпроти, своєю бездіяльністю чи необдуманими діями (знищення лісів, джерел води, забруднення середовища життєдіяльності і ін.) може багаторазово підсилити наявний у природі руйнівний потенціал (рис. В.5).

Екологічні катастрофи викликаються локальними чи планетарними дестабілізуючими функціями біосфери. Найчастіше вони є наслідком дій соціуму на середовище життя, використанням, споживанням природно-ресурсного потенціалу. Зростаючи, тиск людини на природу підриває відбудовну здатність біосфери, її основних ланок і, у кінцевому рахунку, викликає катастрофи локального та глобального масштабу.

а)



б)

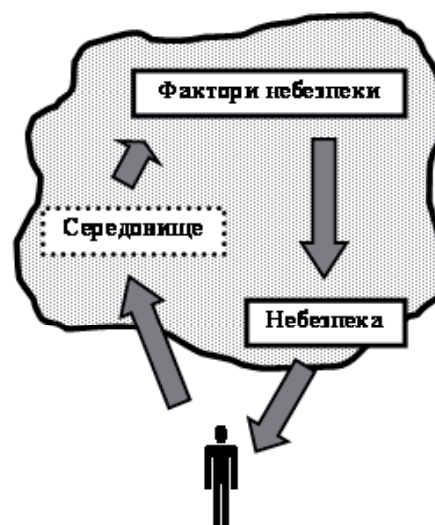


Рис. В.5 – Взаємодія соціуму з природно-техногенно-соціальною системою в умовах надзвичайних ситуацій: а) безпосередній вплив середовища; б) відгук середовища на діяльність соціума

Енергетичні, ядерні, транспортні, інфраструктурні аварії і катастрофи є наслідком неузгодженості взаємодії між елементами системи „людина-машинна”. У цьому типі катастроф, враховуючи постійний розвиток техніки, велику роль

починає відігравати людський фактор – прийняття необґрунтованих рішень на всіх рівнях, інженерні помилки, помилки персоналу, неефективні дії та допомога рятувальних служб [22]. Зростання розмірів та потенціалу технічних систем веде до збільшення масштабів людських, матеріальних і екологічних втрат [23].

Соціальні катастрофи є наслідком непередбаченої чи свідомої цілеспрямованою діяльністю з руйнування соціальних цінностей та державних інститутів, зміни соціально-політичного ладу, знищенню народів, країн, політичних союзів, цивілізацій. Цей тип катастроф веде до великих людських втрат, деградації демографічної і соціальної структур суспільства, руйнуванню духовних основ життя [24 – 26].

Попередження небезпечних процесів може бути ефективним лише за умов отримання своєчасної й об'єктивної оцінки стану систем життєзабезпечення [27]. Для цього з використанням уже досягнутих результатів у природно-техногенно-соціальній сфері необхідно розробити методологію комплексного системного аналізу інтегральних ризиків ПТС систем та пропозицій з управління безпекою в умовах обмеженої та нечіткої інформації. Моніторинг стану ПТС системи і ризиків дозволить не тільки знизити загрози, але і збитки від природних, техногенних та соціально-політичних катастроф. Застосування системного підходу до вирішення задачі безпеки дозволяє розглядати весь комплекс існуючих проблем [28 – 31], що мають місце при виникненні катастрофічних ситуацій.

Аналіз проблем, методів вирішення задачі прогнозування доводить складність системного узагальнення всіх елементів безпеки ПТС систем. При вивченні впливів природних та техногенних катастроф на соціальні системи виявляється не лінійність і різномірність процесів, які відбуваються, при цьому ці властивості характерні як в окремим елементам систем, так і їх комбінаціям [32 – 35].

Вирішення задачі оцінки ризиків надзвичайних ситуацій у ПТС системах потребує розвитку принципово нових методів дослідження, які спираються на критерії інтегральної безпеки з урахуванням властивостей складних систем на різних стадіях виникнення і розвитку надзвичайних ситуацій. Тому виникає необхідність вивчення питань взаємодії різних елементів системи, оцінка стану як окремих підсистем, так і системи в цілому, визначення основних елементів системи і можливості впливу на них і т.д. Слід зазначити, що проблема безпеки

тісно пов'язана з класифікацією регіонів, яка повинна враховувати взаємозв'язок всіх компонентів ПТС системи і відповідних ризиків.

З іншого боку, для побудови системи безпеки ПТС доцільним є використання вже існуючого технічного та економічного потенціалу з попереднім аналізом його ефективності та відповідності принципам інтегральної безпеки.

Однак на сьогодні єдиної класифікації небезпечних чинників, а відповідно понять криз і ризиків у природних, техногенних, соціальних, природно-техногенних, природно-соціальних, соціально-економічних, економічних системах не існує, що ускладнює розробку єдиних підходів до отримання інформації нестійкості таких систем та прийняття відповідних антикризових рішень.

Таким чином, виникає необхідність аналізу умов функціонування природно-техногенно-соціальної системи з територіально-часовим розподілом параметрів – території України, що дозволить у подальшому сформулювати принцип комплексної оцінки безпеки від надзвичайних ситуацій та розкрити його місце у постійному процесі запобігання проявам внутрішніх та зовнішніх небезпек.

**Не існує невдач,
є тільки зворотній зв'язок**

Алдер Херри

1. СИСТЕМА ІНТЕГРАЛЬНОЇ БЕЗПЕКИ ІЗ ЗАПОБІГАННЯ ЕКСТРЕМАЛЬНИХ ТА НАДЗВИЧАЙНИХ СИТУАЦІЙ

1.1. Концепція системи інтегральної безпеки. Основні принципи побудови елементів системи

Сучасний розвиток України, як багатогранної системи з територіально-часовим розподілом параметрів, не виключає можливості прояву та виникнення різного роду екстремальних та надзвичайних ситуацій – природного, техногенного, воєнного та соціально-політичного характеру [36, 37], що в свою чергу потребує докорінного перегляду існуючих підходів до побудови концепції безпеки як сукупності складових інженерно-технічного та соціально-психологічного характеру з невід'ємним урахуванням стрімкого розвитку суспільства.

Про необхідність комплексного підходу до побудови та розвитку систем безпеки свідчать дискусії, що тривають в наукових колах. Втім подібний підхід потребує досить широкої різноплановості досліджень у протилежних сферах знань, що ускладнює формування єдиного цілісного підходу до безпеки об'єктів та примушує дослідників штучно розмежовувати завдання. Так, наприклад, у роботах [38 – 40] розглядаються питання підвищення ефективності виявлення небезпечних факторів та ліквідації НС. Однак ці дослідження стосуються лише інженерно-технічного боку процесу забезпечення безпеки.

У роботах [19, 20, 41 – 45] відображено результати досліджень у соціально-психологічному аспекті даної проблеми. Мова йде переважно про проміжок часу коли надзвичайна ситуації вже трапилась, тобто дослідження поведінки соціуму у екстремальних ситуаціях, питання впливу соціально-психологічних показників на процес виникнення НС у комплексному вигляді майже не розглядаються.

Таким чином, питання щодо взаємного впливу різних аспектів та їх впливу на показники інтегральної системи безпеки при надзвичайних ситуаціях досі залишається не вирішеними, незважаючи на окремі положення, які знайшли

відображення в роботах Полікарпова В.С., Бро Г.В., Буркова В.Н. та інші [46 – 50].

Запропонований підхід до розгляду системи безпеки (рис. 1.1), дозволяє не тільки розкрити її сутність та складові, але й визначити її місце і роль у постійному процесі запобігання проявам небезпечних факторів аварій та надзвичайних ситуацій.



Рис. 1.1 – Концепція системи інтегральної безпеки

Аналіз загальної схеми системи інтегральної безпеки (СІБ) доводить необхідність розробки останньої як суми інтегральних складових ($S_k^{i,j}$) – рис. 1.2, з урахуванням впливу цих складових по двом напрямках: інженерно-технічному

(i) та соціально-психологічному (j):
$$F_{SB} = \sum_{i=0}^n \sum_{j=0}^m f(S_1^{i,j} \dots S_k^{i,j}).$$

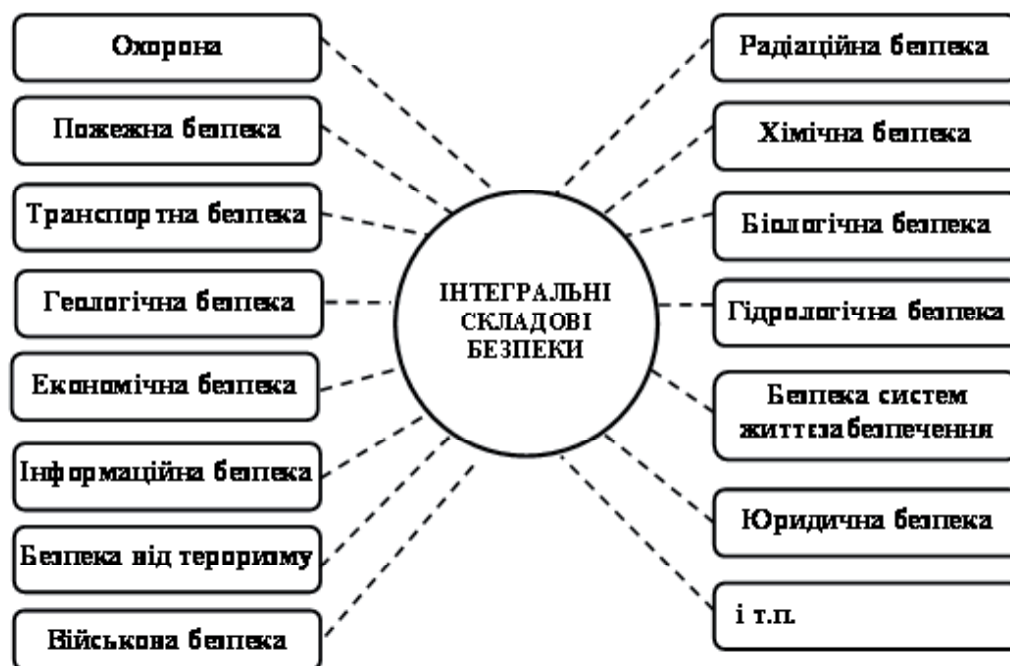


Рис. 1.2 – Інтегральні складові безпеки

Кожна складова СІБ ($S_k^{i,j}$) – рис. 1.3, повинна об'єднувати напрямки існуючих заходів з попередження прояву небезпеки ($\Pi_k^{i,j}$) та прогнозуємих заходів з її ліквідації ($L_k^{i,j}$) – $S_k^{i,j} = \Pi_k^{i,j} + L_k^{i,j}$. Останні потребують необхідності розробки як організаційно-оперативних заходів, так і технічних засобів, об'єднання яких дозволить забезпечити необхідний рівень безпеки (B).

Аналізуючи структуру елементів СІБ слід зазначити, що для кожного об'єкту необхідно розробляти свою систему безпеки, а відповідно і впливи інженерно-технічної та соціально-психологічної складових у систему безпеки різних об'єктів будуть різні. Збільшуючи інженерно-технічну складову ми зменшуємо соціально-психологічний внесок (% - впливу на систему безпеки зв'язків «людина-машина» та «людина-людина») і відповідно ймовірність виникнення НС які пов'язані з людським фактором. Однак ускладнення та додаткове застосування технічних засобів безпеки призводить до виникнення перенавантаження оператора або спеціаліста з безпеки, що, у свою чергу, зменшує ефективність роботи останніх з прийняття адекватних рішень, які є кінцевим елементом системи безпеки, як на рівні окремих об'єктів, так і на рівні загальнодержавної системи безпеки.

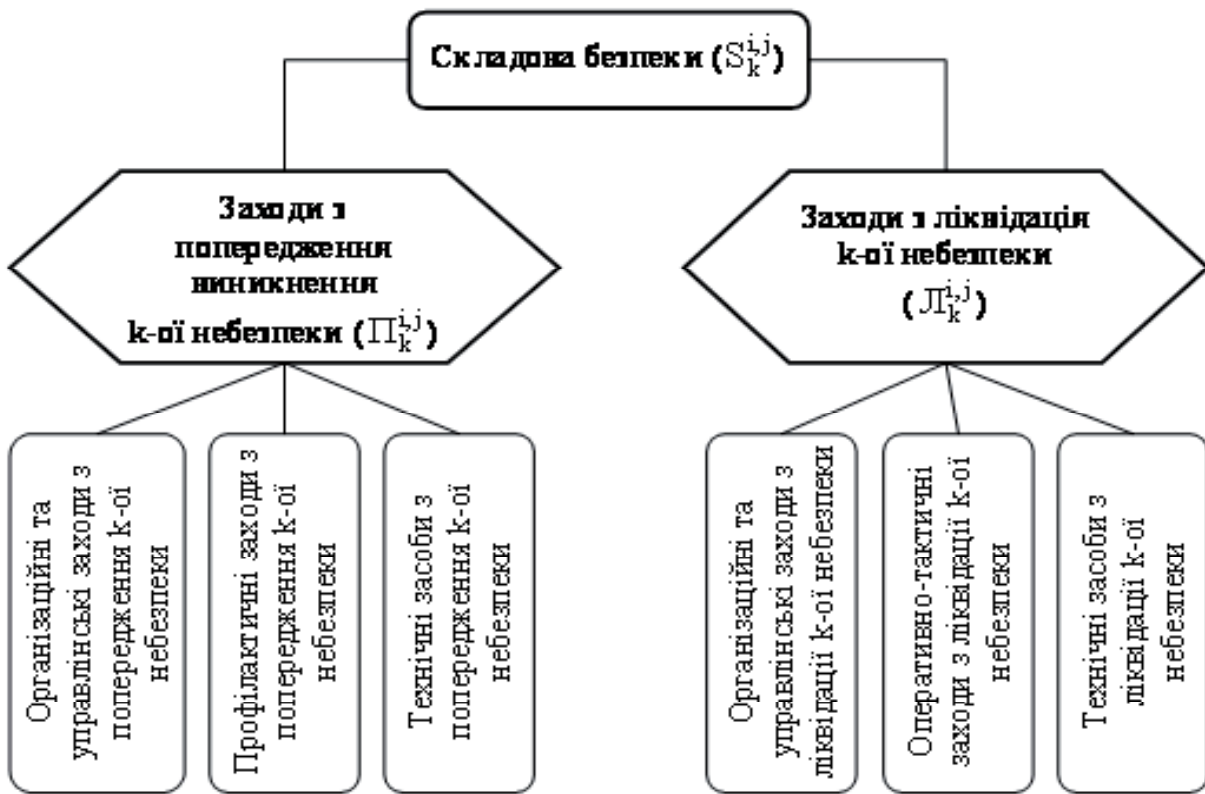


Рис. 1.3 – Структура заходів елементу системи інтегральної безпеки

Висновок: обидва напрямки елементів СІБ (інженерно-технічний та соціально-психологічний) повинні розвиватися з урахування особливостей об’єкту безпеки, з використанням в якості кінцевого елементу – інтелектуальних підсистем з прийняття рішень, які здатні зменшити «управлінське» навантаження на оператора.

1.2. Функції та структура системи інтегральної безпеки

Основна функція СІБ від надзвичайних ситуацій полягає в раціональному розподілі сил і засобів для запобігання і ліквідації наслідків функціонування об’єкту захисту (ОЗ) в режимі виникнення небезпечної ситуації.

Представлена на рис. 1.4 схема розкриває умови функціонування відповідної системи безпеки. Вплив на об’єкт захисту факторів різного походження ($P_1 \div P_n$)

– природні чинники; $T_1 \div T_m$ – техногенні чинники; $S_1 \div S_d$ – соціально-політичні чинники; $V_1 \div V_k$ ($n \neq m \neq d \neq k$) формують сукупність чинників небезпеки

$$F_P = \sum_{i=1}^n P_i, F_T = \sum_{j=1}^m T_j, F_S = \sum_{q=1}^d S_q, F_V = \sum_{w=1}^k V_w, \text{ які призводять у свою чергу до ви-}$$

никнення нерегламентованої ситуації $F_{NS} = F_P + F_T + F_S + F_V$.

Прояви останніх призводять до відхилень від нормального функціонування ОЗ. Відповідно до рівня ОЗ, наслідки таких дій негативно позначається на життєзабезпеченні, економіці, соціальній сфері, природному середовищі і призводить до зниження рівня безпечного функціонування об'єкту захисту.

Виключення переходу ОЗ у стан нерегламентованого режиму функціонування – основне завдання СІБ, а за умови його виникнення – проведення антикризових заходів G_{SB} з метою мінімізації часу функціонування в нерегламентованих режимах, а у разі неможливості стабілізації ОЗ, проведення заходів направлених на зменшення соціального та матеріального збитку.

Визначення ефективності системи безпеки можливо шляхом введення показника рівня захисту об'єкту (території) наступним чином:

$$B = \frac{F_{NS}}{G_{SB}}, \quad (1.1)$$

де G_{SB} – інтегральний показник системи безпеки; F_{NS} – інтегральний показник небезпеки

$$F_{NS} = f(N_P, N_T, N_S, N_V, U_P, U_T, U_S, U_V), \quad (1.2)$$

де N_P, N_T, N_S, N_V – збитки від природних (P), техногенних (T), соціально-політичних (S) та воєнних (V) небезпек; U_P, U_T, U_S, U_V – ймовірність виникнення P, T, S, V небезпек.

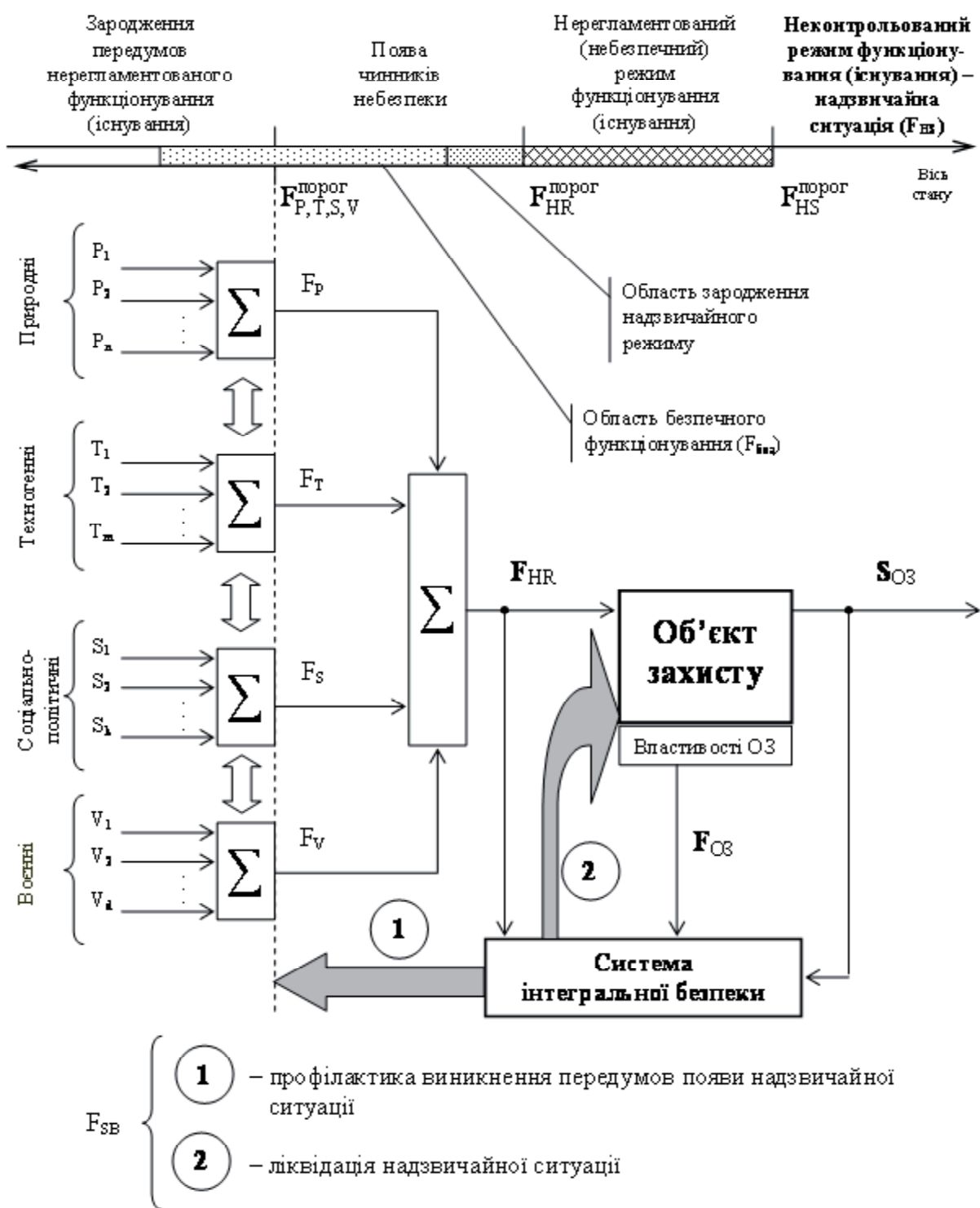


Рис. 1.4 – Загальна схема функціонування системи інтегральної безпеки об'єкту захисту [51]: P_p, T_j, S_q, V_w – природні, техногенні, соціально-політичні, воєнні чиники; F_p, F_t, F_s, F_v – чинники небезпеки природного, техногенного, соціально-політичного, воєнного характеру; F_{HR} – небезпечний режим; F_{O_3} – властивості об'єкту захисту; S_{O_3} – стан ОЗ; F_{SB} – функції системи безпеки.

Показник системи безпеки виступає функцією наступних показників другого рівня:

$$G_{SB} = f(G_{\text{Тактич.}}, G_{\text{Техн.}}, G_{\text{Соц.}}, G_{\text{Екон.}}), \quad (1.3)$$

де $G_{\text{Тактич.}}$, $G_{\text{Техн.}}$, $G_{\text{Соц.}}$, $G_{\text{Екон.}}$ – тактичний, технічний, соціальний, економічний показники ефективності системи безпеки.

Основні задачі, які повинна вирішувати СІБ об'єкту захисту, це на I етапі – збір, обробка інформації про джерела небезпеки; формування та прийняття рішень, які унеможливають перехід ОЗ в стан небезпечного функціонування, а у разі незворотності (II етап) – мінізація часу та необхідних зусиль на подолання наслідків неконтрольованого режиму функціонування, формування рекомендацій щодо зниження наслідків НС; управління службами підтримки та відновлення життєдіяльності в кризових ситуаціях; на III етапі – аналіз причин та існуючих недоліків, удосконалення функціональної структури СІБ (зворотній зв'язок). Наявність II етапу – чіткий індикатор існуючих недоліків СІБ, які повинні бути усунуті в процесі її розробки, формування та пілотної експлуатації. Заходи III етапу повинні проводитися планово у разі відсутності II етапу та позачергово у разі виникнення II етапу функціонування системи інтегральної безпеки.

Для вирішення поставлених задач система безпеки повинна об'єднувати підсистему отримання (ПОт.І) та підсистему обробки (ПОб.І) інформації (рис. 1.5).

Об'єкт захисту зазнає впливу різних зовнішніх факторів $\xi_i(t)$ ($i = 1 \dots N$). Інформація о параметрах S_{O3} може бути отримана за допомоги методів та засобів контролю λ_j ($j = 1 \dots M$), які складають підсистему отримання інформації. На функціональному рівні ПОт.І об'єднує підсистеми контактної та дистанційної контролю, які в залежності від умов використання та розміщення поділяються на космічні, повітряні, морські та наземні.

Інформація через засоби комунікації надходить до аналітичного органу системи – підсистемі обробки інформації та формування управлінського рішення. Основним завданням ПОб.І є можливість прогнозу небезпек та відповідно розробки рекомендацій щодо зниження рівня впливу небезпечних факторів на об'єкт

захисту.

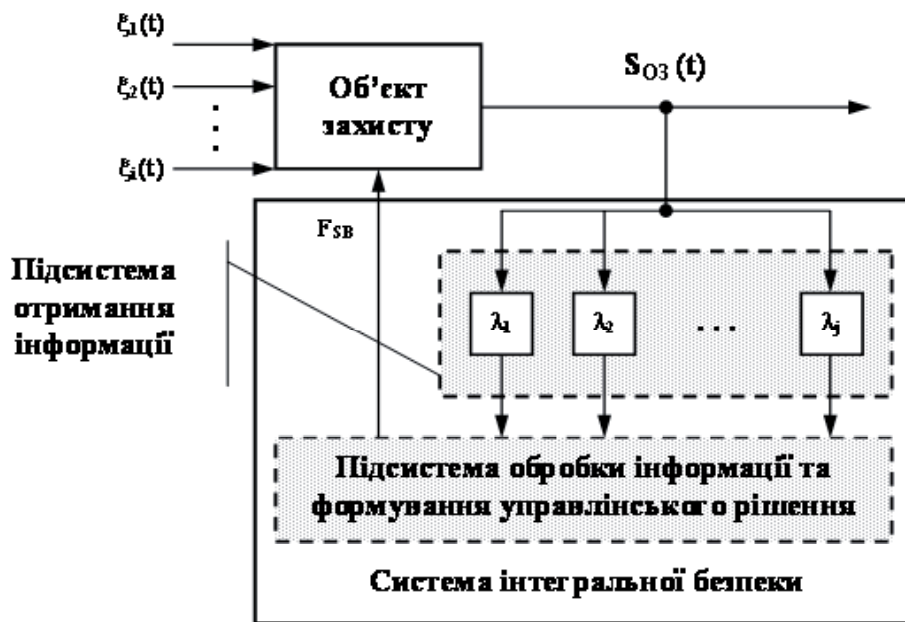


Рис. 1.5 – Функціональна схема підсистем I етапу системи інтегральної безпеки об'єкту захисту

З позиції системного аналізу до двох вже зазначених підсистем системи інтегральної безпеки I етапу функціонування:

- підсистему спостереження і контролю;
- підсистему збору, обробки фактичної інформації, прогнозування небезпеки та управління в кризових ситуаціях

слід додати підсистему II етапу:

- підсистему ліквідації надзвичайних ситуацій (неконтрольованих режимів функціонування)

та підсистему III етапу:

- підсистему аналізу та удосконалення СІБ (рис. 1.6).

Специфіка вирішуваних завдань, що стоять перед системою моніторингу, накладає ряд вимог на її функціонування [52].

В цілому вимоги до підсистеми отримання інформації передбачають:

- оснащення ПОт.І різнофункціональними носіями засобів спостереження за джерелами надзвичайних ситуацій;

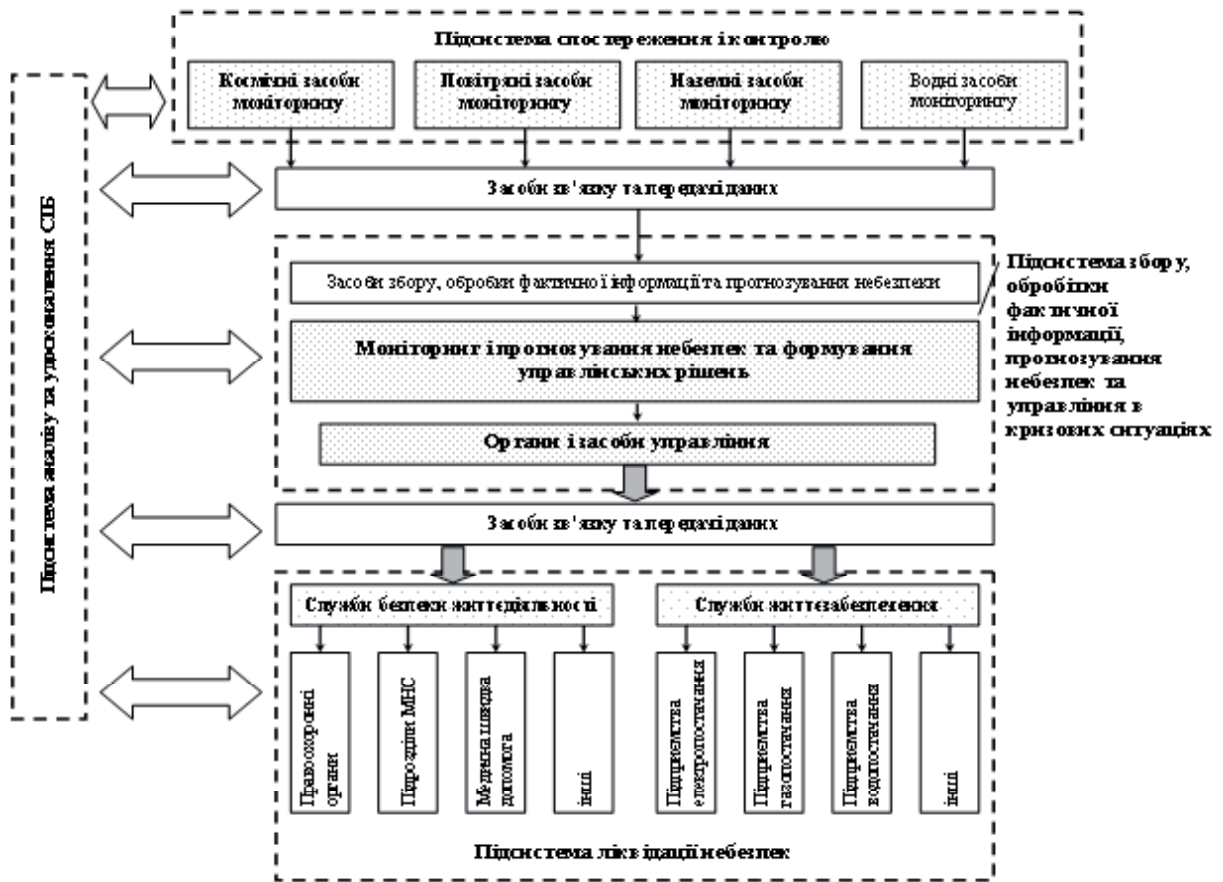


Рис. 1.6 – Структурна схема системи інтегральної безпеки

- наявність сучасних вимірювальних засобів і лабораторних (стаціонарних і мобільних) комплексів, що функціонують на єдиній елементній базі;
- автономність і надійність функціонування вузлів системи в будь-яких (гідрометеорологічних, хімічно і радіаційно небезпечних) умовах;
- оптимальний просторово-часовий розподіл засобів моніторингу відповідно до обґрунтованого підходу до щільності мережі спостереження за джерелами надзвичайних ситуацій;
- забезпечення носіїв засобів спостереження необхідними засобами зв'язку, що забезпечують передачу фактичної інформації в реальному масштабі часу або максимально наближеному до нього.

Основні вимоги до підсистеми обробки інформації включають:

- можливість створення нерегламентованих запитів. Не дивлячись на те, що частина запитів до системи на обробку інформації буде регламентована за часом надходження, складом і структурою вихідної

- (вторинної) інформації, велика кількість запитів не піддається регламентації. Кожен з цих запитів може включати декілька складових обробки з великим потоком проміжної інформації, необхідної як для даного запиту, так і для інших запитів. У цій ситуації процес обробки розчленовується на велике число елементів, які обмінюються між собою інформаційними масивами різної структури і величини. Велике число елементів і різноманітних структур даних, що передбачається, в умовах нерегламентованих запитів веде до розгляду завдання автоматичного планування розрахунків з метою задоволення цих запитів;
- оперативний зв'язок з банком даних. При виконанні запитів вихідна інформація поступатиме з банку даних. При цьому необхідне повне узгодження як за складом, так і за структурою інформації, що зберігається в банку даних і курсує між окремими процесами обробки. Крім того, необхідно забезпечити швидкий доступ до інформації в банку даних з боку оброблювальних програм;
 - багатоваріантність обробки. Як правило, один і той же запит може бути задоволений різними способами залежно від вибору альтернативних моделей. Альтернативи виникають за наявності моделей, заснованих на різних гіпотезах, необхідній точності, деталізації, наявності необхідної і вихідної інформації. Обробка повинна налаштовуватися на необхідні альтернативи як автоматично, так і на вимогу (вказівку) користувача системи;
 - постійний процес мінімізації часу аналізу. Зважаючи на специфіку даної системи, в певних умовах ця характеристика набуває особливої значущості. Необхідно забезпечити постійне скорочення часу планування, автоматичних розрахунків і розрахунків за вказівкою користувача;
 - можливість розподіленої обробки. Система повинна передбачати наявність значної кількості зв'язаних між собою центрів збору, обробки і розповсюдження інформації як дублюючих один одного в необхідних межах, так і таких, що мають власну специфіку функціонування;

- функціональну гнучкість програмного забезпечення. Однією з найважливіших вимог до програмного забезпечення ПОБ.І є забезпечення постійної модернізації. Передбачається, що в процесі функціонування системи постійно збільшуватиметься кількість запитів, що, у свою чергу, вимагатиме вдосконалення програм обробки і розрахунку необхідної інформації за запитами споживачів;
- створення роздільного доступу. Система передбачає наявність великого числа користувачів, які мають право одночасного доступу до банку даних. У зв'язку з цим кожний центр обробки інформації необхідно забезпечити режимом розподілу доступу між багатьма терміналами користувачів, кожен з яких може мати свою специфіку. Все це накладає додаткові вимоги до програмного забезпечення центрів обробки і термінальних станцій;
- можливість роботи в інтерактивному (діалоговому) режимі. Використання режиму розділення доступу як основного режиму роботи системи має на увазі інтерактивний режим спілкування з нею в процесі її підтримки і експлуатації. Той факт, що в процесі спілкування з системою будуть брати участь різні користувачі (розробники, обслуговуючий персонал тощо) з різним рівнем кваліфікації, вимагає створення програмного забезпечення, що дозволяє легко перебудувати мову і форму діалогу відповідно до вимог, що змінюються. Необхідно зважати на специфіку регіональних і територіальних центрів моніторингу і прогнозування надзвичайних ситуацій, специфіку завдань і роботи операторів з одного боку, і структуру спілкування в рамках всієї системи з іншою.
- можливість відображення інформації. Відображення інформації в зручній для користувача формі є ключовим моментом взаємодії людини із складними комп'ютерними комплексами. Дане завдання характеризується великою різноманітністю очікуваних форм представлення інформації про надзвичайні ситуації і їх джерела (таблиці, графіки, мапи). Все це вимагатиме розробки спеціального програмного забезпечення, погодженого з функціонуванням в інтерактивному режимі.

Як бачимо, створення єдиної системи моніторингу – складне багаторівневе завдання, яке передбачає використання останніх наукових досягнень як в області забезпечення безпеки життєдіяльності суспільства, так і в області телекомунікацій і програмного забезпечення.

1.3. Принцип комплексної оцінки інтегральної безпеки об'єктів захисту регіонального рівня

Умови функціонування регіональної територіально-часової параметричної підсистеми представлено на рис. 1.7. Аналіз дозволяє сформувати принцип комплексної оцінки стану інтегральної безпеки ОЗ регіонального рівня та розкрити його місце у постійному процесі запобігання проявам внутрішніх та зовнішніх небезпек.

Аналіз взаємозв'язку внутрішніх та зовнішніх небезпек сталого функціонування державної територіально-часової параметричної системи (ДТЧПС), до складу якої входять природно-технічно-соціальні підсистеми наведено у табл. 1.1. До природно-технічно-соціальних підсистем слід віднести як об'єкт захисту з існуючою системою безпеки від НС, так і самі можливі небезпеки.

Таблиця 1.1 – Взаємозв'язок природно-технічно-соціальних підсистем в ДТЧПС

	Середовище функціонування ОК	Об'єкт контролю	Система безпеки
Зовнішні небезпеки	безпосередній вплив	$\epsilon_{CB} \epsilon_0$	ϵ_0
Внутрішні небезпеки	$\epsilon_{OK} \epsilon_{CB}$	безпосередній вплив	ϵ_{OK}

Аналіз взаємозв'язку розглянутих підсистем ДТЧПС дозволяє сформувати принцип комплексної оцінки стану безпеки ОЗ шляхом введення інтегрального показнику ефективності відгуку ДТЧПС в умовах НС (${}^{(ДТЧПС)}K_m^{небезп.}$), а саме коефіцієнту небезпеки окремих складових (і-тих регіонів – ${}^{(i)}K_m^{небезп.}$) який має наступний вигляд:

$${}^{(i)}K_m^{\text{небезп.}} = \frac{\sum_{i=1}^n {}^{(i)}K_m^{\text{небезп.}}}{n}; \quad (1.4)$$

$${}^{(i)}K_m^{\text{небезп.}} = f\left({}^{(i)}k_m^{\text{техн.}}; {}^{(i)}k_m^{\text{прир.}}; {}^{(i)}k_m^{\text{соц.-політ.}}; {}^{(i)}k_m^{\text{воєн.}}\right),$$

де ${}^{(i)}k_m^{\text{техн.}}$, ${}^{(i)}k_m^{\text{прир.}}$, ${}^{(i)}k_m^{\text{соц.-політ.}}$, ${}^{(i)}k_m^{\text{воєн.}}$ – показники небезпек: техногенного, природного, соціально-політичного, воєнного характеру [16] i -го регіону; n – кількість регіонів, що входить до складу ДТЧПС; m – стан системи – рис. 1.8.

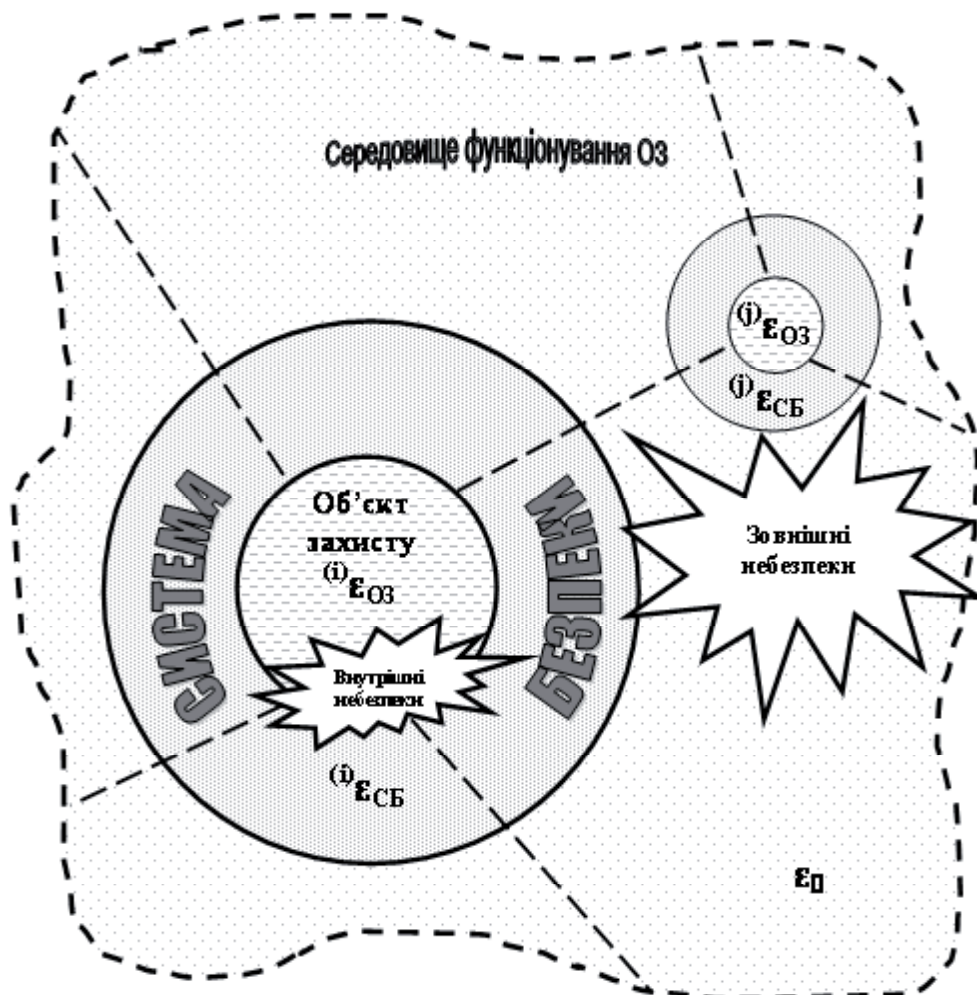


Рис. 1.7 – Концептуальна схема функціонування інтегральної системи безпеки від надзвичайних ситуацій (ϵ_0 ; ϵ_{OK} ; ϵ_{CB} – властивості: середовища в якому функціонує об'єкт; об'єкту контролю (ОК); системи безпеки від НС)

Показники небезпек можливо представити наступним чином:

$${}^{(i)}K_m^\lambda = f\left({}^{(i)}\alpha_m^\lambda; {}^{(i)}\beta_m^\lambda; {}^{(i)}\chi_m^\lambda; {}^{(i)}\mu_m^\lambda; {}^{(i)}\varphi_m^\lambda; {}^{(i)}S_m^\lambda; {}^{(i)}N_m^\lambda; {}^{(i)}N_{\lambda_m}^{\text{насел.}}; {}^{(i)}U_m^\lambda\right), \quad (1.5)$$

де λ – вказівний небезпеки згідно (1.4); ${}^{(i)}\alpha_m^\lambda$, ${}^{(i)}\beta_m^\lambda$, ${}^{(i)}\chi_m^\lambda$, ${}^{(i)}\mu_m^\lambda$ та ${}^{(i)}\varphi_m^\lambda$ – технічні, природні, соціальні (економічні, правові, політичні та інші), індивідуально-фізіологічні (психологічні, медичні та інші) чинники та показник ефективності стану підсистем безпеки та моніторингу λ небезпеки; ${}^{(i)}S_m^\lambda$ – територіально-географічний показник; ${}^{(i)}N_m^\lambda$, ${}^{(i)}U_m^\lambda$ – показники кількості НС λ характеру, що відбулися за аналізуємий час функціонування системи – $m(T_{\text{монитор.}})$, та відповідні втрати від них; ${}^{(i)}N_{\lambda_m}^{\text{насел.}}$ – показник кількості населення, яке має взаємовідношення до НС λ характеру.

Аналіз існуючого стану систем безпеки регіонів України, з урахуванням принципу комплексної оцінки безпеки, за складовими небезпеки техногенного ($\lambda = \text{"техн."}$) та природного ($\lambda = \text{"прир."}$) характерів дозволив, не обмежуючи загальності підходу (1.5), представити останні для i -го регіону наступним чином:

$${}^{(i)}K_m^{\text{техн.}} = {}^{(i)}N_m^{\text{техн.*}} \cdot \frac{{}^{(i)}N_m^{\text{насел.*}}}{{}^{(i)}S_m^*} \cdot {}^{(i)}K_m^{\text{техн.*}} \cdot {}^{(i)}U_m^{\text{техн.*}}, \quad (1.6)$$

де ${}^{(i)}N_m^{\text{техн.*}} = \frac{{}^{(i)}N_m^{\text{техн.}}}{\sum_i {}^{(i)}N_m^{\text{НС}}}$ – відносна кількість НС техногенного характеру, що виникло у i -му регіоні;

${}^{(i)}N_m^{\text{техн.}}$ – кількість НС техногенного характеру у i -му

регіоні; $\sum_i {}^{(i)}N_m^{\text{НС}}$ – загальна кількість НС, що виникло в Україні;

$${}^{(i)}N_m^{\text{насел.}*} = \frac{{}^{(i)}N_m^{\text{насел.}}}{\sum_i {}^{(i)}N_m^{\text{насел.}}} - \text{відносна кількість населення у } i\text{-му регіоні; } {}^{(i)}N_m^{\text{насел.}} -$$

кількість населення у } i\text{-му регіоні; } \sum_i {}^{(i)}N_m^{\text{насел.}} - \text{загальна кількість населення}

$$\text{України; } {}^{(i)}S_m^* = \frac{{}^{(i)}S_m}{\sum_i {}^{(i)}S_m} - \text{відносна площа території } i\text{-го регіону; } {}^{(i)}S_m - \text{ площа}$$

території } i\text{-го регіону; } \sum_i {}^{(i)}S_m - \text{загальна площа території України;}

$${}^{(i)}U_m^{\text{техн.}*} = \frac{{}^{(i)}U_m^{\text{техн.}}}{\sum_i {}^{(i)}U_m^{\text{техн.}}} - \text{відносний показник втрат від НС техногенного характе-}$$

ру у } i\text{-му регіоні; } {}^{(i)}U_m^{\text{техн.}} - \text{втрати від НС техногенного характеру у } i\text{-му регіоні;}

$\sum_i {}^{(i)}U_m^{\text{техн.}}$ – загальні втрати від НС техногенного характеру в Україні;

$${}^{(i)}K_m^{\text{техн.}*} = f\left({}^{(i)}\alpha_m^{\text{техн.}}; {}^{(i)}\beta_m^{\text{техн.}}; {}^{(i)}\chi_m^{\text{техн.}}; {}^{(i)}\mu_m^{\text{техн.}}; {}^{(i)}\phi_m^{\text{техн.}}; {}^{(i)}S_m^{\text{техн.}}\right) - \text{коефіцієнт, який}$$

відображає властивості } i\text{-го регіону України за техногенною небезпекою з ура-
хуванням чинників – (1.5).

Складова безпеки природного характеру } i\text{-го регіону:

$${}^{(i)}K_m^{\text{прир.}} = {}^{(i)}N_m^{\text{прир.}*} \cdot \frac{{}^{(i)}N_m^{\text{насел.}*}}{({}^{(i)}S_m^*)} \cdot {}^{(i)}K_m^{\text{прир.}*} \cdot {}^{(i)}U_m^{\text{прир.}*}, \quad (1.7)$$

$$\text{де } {}^{(i)}N_m^{\text{прир.}*} = \frac{{}^{(i)}N_m^{\text{прир.}}}{\sum_i {}^{(i)}N_m^{\text{НС}}} - \text{відносна кількість НС природного характеру, що виникло}$$

у } i\text{-му регіоні; } {}^{(i)}N_m^{\text{прир.}} - \text{кількість НС природного характеру у } i\text{-му регіоні;}

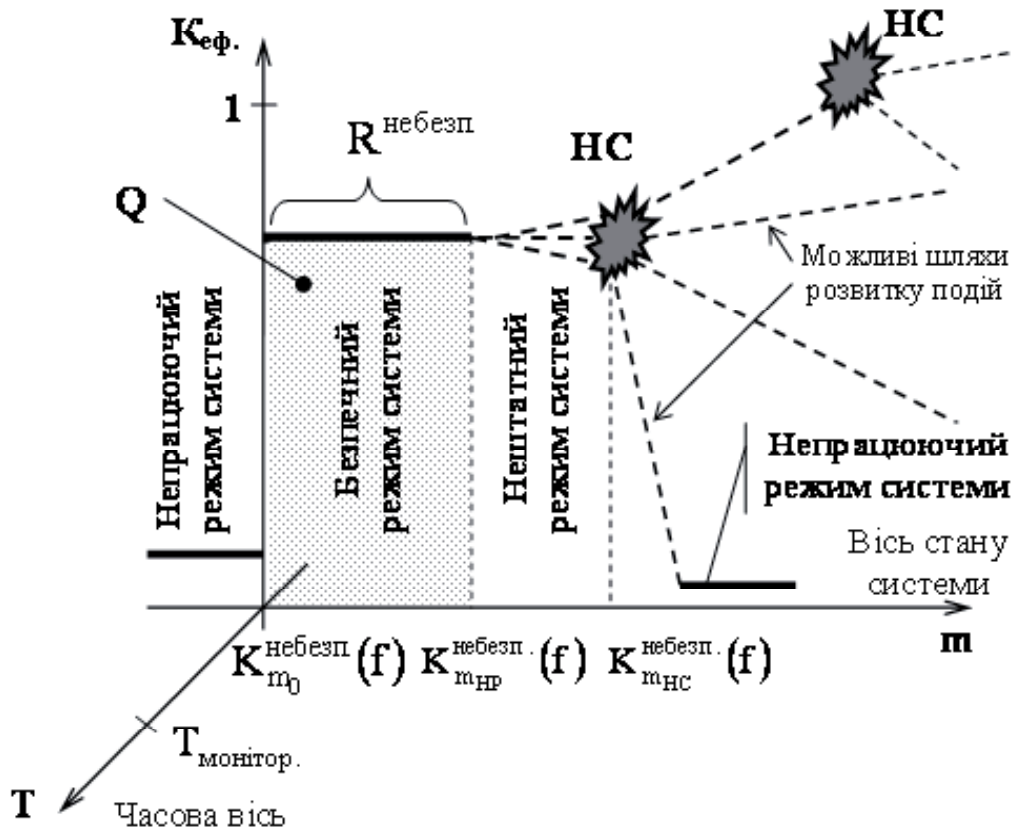


Рис. 1.8 – Відносно-часове відображення режимів функціонування ДТЧПС ($K_{эф.}$ – коефіцієнт ефективності функціонування системи; $Q(K_{эф.}; R^{небезп.})$ – надійності системи; $R^{небезп.}$ – ризик небезпеки ($10^{-10} \div 10^{-4}$ [53]); $K_{m_0}^{небезп.}(f)$ – показник небезпеки системи на початковому етапі функціонування m_0 ; $K_{m_{нр}}^{небезп.}(f)$ – показник небезпеки системи у нештатному режимі $m_{нр}$; $K_{m_{нс}}^{небезп.}(f)$ – показник небезпеки системи в умовах надзвичайної ситуації $m_{нс}$; $T_{монитор.}$ – часова точка проведення поточного моніторингу функціонування системи)

$$\sum_i^{(i)} N_m^{НС} \text{ – загальна кількість НС, що виникло в Україні; } {}^{(i)} U_m^{прир.*} = \frac{{}^{(i)} U_m^{прир.}}{\sum_i {}^{(i)} U_m^{прир.}}$$

– відносний показник втрат від НС природного характеру у i -му регіоні; ${}^{(i)} U_m^{прир.}$ –

втрати від НС природного характеру у і-му регіоні; $\sum_i^{(i)} U_m^{\text{прир.}}$ – загальні втрати

від НС природного характеру в Україні;

$^{(i)}k_m^{\text{прир.*}} = f\left(^{(i)}\alpha_m^{\text{прир.}}; ^{(i)}\beta_m^{\text{прир.}}; ^{(i)}\chi_m^{\text{прир.}}; ^{(i)}\mu_m^{\text{прир.}}; ^{(i)}\phi_m^{\text{прир.}}; ^{(i)}S_m^{\text{прир.}}\right)$ – коефіцієнт, який

відображає властивості і-го регіону України за природною небезпекою з урахуванням чинників – (1.5). Результати якісного аналізу з наведених складових докладно розглянуті у другому розділі роботи.

1.4. Принцип комплексної оцінки стану інтегральної безпеки об'єктового рівня

Загальна структурна схема об'єктової системи інтегральної безпеки представлена на рис. 1.9 [54, 55]. Ця система забезпечує рішення наступних задач:

- захист життя і здоров'я людей;
- захист матеріальних та інформаційних цінностей;
- захист власних ресурсів і т.п.

До складу системи входять підсистеми забезпечення безпеки, життєзабезпечення та зв'язку.

Система інтегральної безпеки буде тим більш ефективною, чим більш вона конкретизована (забезпечує захист конкретного об'єкту від конкретних небезпек). Таким чином, етапу проектних та монтажних робіт, встановлення техніки і т.п. повинен передувати етап конкретизації та уточнення підсистем та елементів СІБ, яка необхідна для забезпечення сталого рівня роботи підприємства. Для досягнення зазначеної мети необхідно вирішити наступні питання:

- визначити цілі захисту та їх пріоритети;
- визначити види, способи реалізації та наслідки загроз;
- визначити вимоги до елементів та підсистем СІБ.

Таким чином, постає питання необхідності проведення систематичного аналізу мір по забезпеченню безпеки функціонування ОЗ, який прийнято називати аналізом вразливості (АВ) [56 – 60].

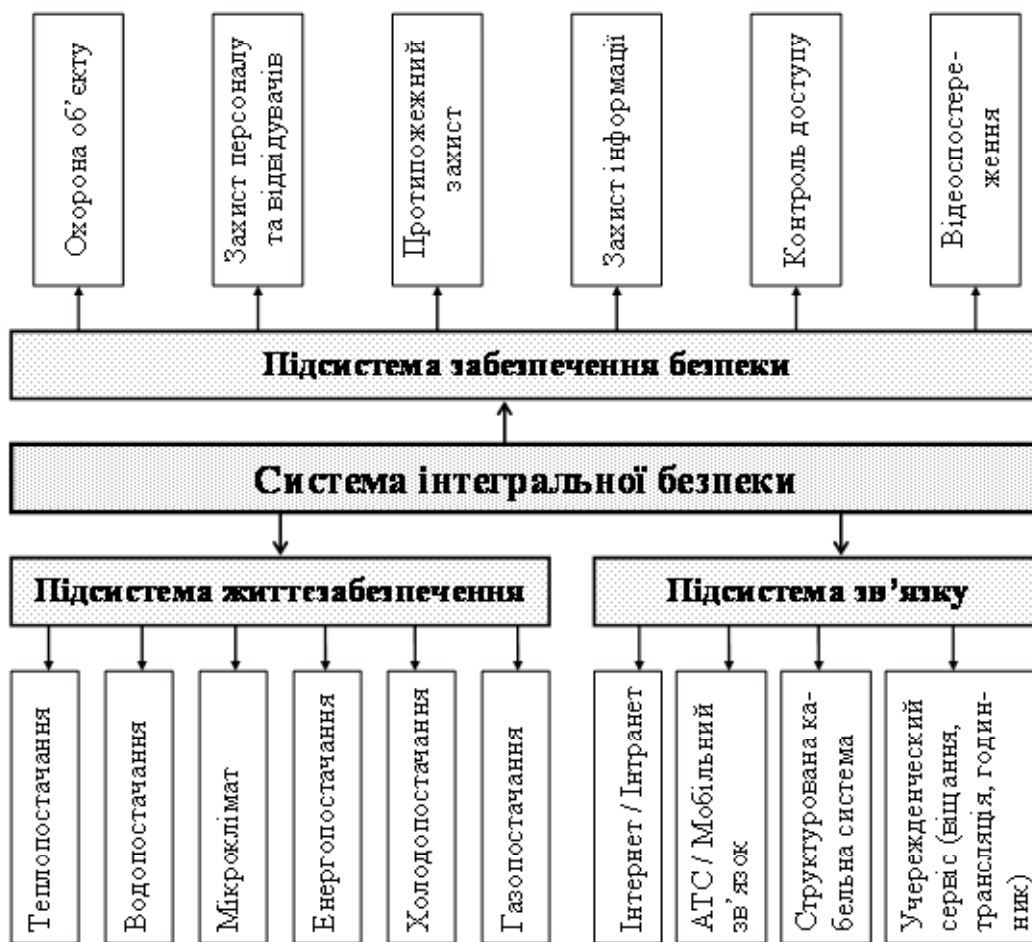


Рис. 1.9 – Об'єктова система інтегральної безпеки

Основною ціллю проведення АВ є визначення внутрішніх та зовнішніх загроз, а також виявлення вразливих місць ОЗ з метою створення або модернізації, на основі отриманої інформації, ефективної системи інтегральної безпеки.

Втім, тільки маючи достатні, чіткі та якісні данні, можливо оцінити ефективність існуючої СІБ, обґрунтувати доцільність її удосконалення, вказати основні напрямки такої роботи, оцінити проектні пропозиції і т.п. Зазвичай відповідний масив даних можливо отримати користуючись методом експертних оцінок або методом математичного моделювання.

Експертний аналіз вразливості об'єкту захисту дозволяє на основі суджень експертів визначити і ранжирувати небезпеки, способи і наслідки їх виникнення при фактичному стані системи інтегральної безпеки. Цей метод можливо використовувати при визначенні цілій захисту, що дозволить виділити найбільш значимі

або пріоритетні структурні одиниці об'єкту та оцінити їх вразливість. Формування відповідних критеріїв оцінки дозволить також зробити якісний аналіз стану системи інтегральної безпеки ОЗ та виділити основні напрямки її удосконалення. Таким чином, метод експертних оцінок призначений для прийняття принципового рішення про необхідність модернізації або, у випадку необхідності, створення додаткової СІБ.

Аналіз на основі математичного моделювання, переважно застосовується з використанням просторових моделей, дозволяє також виділити небезпеки, які суттєво впливають на функціонування підприємств і розрахувати їх тимчасові і вірогідності показники. Порівняння отриманих у такий спосіб даних з заданими критеріями ефективності системи дозволяє не тільки розробити певні вимоги до створення системи інтегральної безпеки, а й і оптимізувати її за вартісними показниками. Однак, переваги даного підходу очевидні лише при наявності великої бази статистичних даних про стан і функціонування об'єкту захисту. Враховуючи відсутність системного накопичення та висвітлення даних, слід застосовувати для встановлення коефіцієнтів важливості факторів небезпек функціонування ОЗ метод оцінки усередненої думки експертів.

В основу покладено метод оцінки середньозважених значень визначаємих коефіцієнтів по оцінкам, які надані експертами. У розрахунок вагового коефіцієнта конкретного експерта покладено розрахунок суми квадратів відхилень запропонованих їм значень від середніх значень, отриманих у результаті аналізу усіх результатів – більш вищий ваговий коефіцієнт має відповідно той експерт, у якого результати менше відрізняються від середніх значень.

Щоб нагромадити вихідні дані, які необхідні для експертної оцінки, доцільно використовувати спеціальну форму, у якій визначається коефіцієнт W_{ij} , де i -ий приймає значення $1, \dots, k$ (k – кількість експертів) експерт вважає за доцільне виділити засобів для попередження або ліквідації j – коефіцієнт небезпеки ($j = 1, \dots, l$, де l – кількість небезпек, що можуть вплинути на функціонування об'єкту захисту).

Це має аналогією з підходом, викладеним у [61], де для оцінки середньозваженого коефіцієнту використовуються вагові коефіцієнти експертів. Обробку результатів експертного опитування доцільно проводити в наступній послідовності.

Провести розрахунок величин середнього значення засобів, які пропонується виділити для попередження або ліквідації j -ої небезпеки

$$\bar{w}_j = \frac{\sum_{i=1}^k w_{ij}}{k}. \quad (1.8)$$

Наступним етапом провести розрахунок суми квадратів відхилень по кожній із передбачуваних небезпек між коефіцієнтом w_{ij} , який пропонує i -ий експерт, і його середнім значенням \bar{w}_j

$$S_i = \sum_{j=1}^l (w_{ij} - \bar{w}_j)^2. \quad (1.9)$$

Далі проводиться визначення усередненої думки експертів для встановлення середнього значення вагового коефіцієнту засобів, необхідних для організації заходів з попередження або ліквідації j -ої небезпеки об'єкту захисту. Оцінка усередненого очікуваного значення коефіцієнту здійснюється шляхом підсумовування середньозваженого значення за спостереженнями всіх експертів

$$\tilde{w}_j = \sum_{i=1}^l P_i w_{ji}, \quad (1.10)$$

де $P_i = \frac{S_i}{S_0}$ – вагові коефіцієнти i -го експерта; S_0 – постійна, котра вибирається за

умов:

$$\sum_{i=1}^k S_i = 1, \quad (1.11)$$

тобто

$$S_0 = \frac{1}{\sum_{i=1}^k \frac{1}{S_i}}. \quad (1.12)$$

З метою виключення з загального числа таких оцінок, що мають аномальний вигляд, можливе проведення багатоетапної процедури дельфійського методу вирівнювання індивідуальних оцінок експертів і приведення їх до відповідного загального показника [62]. Для цього проводиться аналіз отриманих оцінок і виділення експертів, які дали оцінки, які різко відрізняються від загальної маси.

1.5. Принцип комплектування технічними засобами системи інтегральної безпеки

Сучасний розвиток техніко-економічних взаємовідношень з одного боку, та низька ефективність використання можливостей вже існуючих технічних засобів з попередження аварій та надзвичайних ситуацій з іншого ставить перед спеціалістами з розробки систем безпеки ряд економічних, організаційних та технічних проблем пов'язаних насамперед з визначенням критеріїв з урахуванням яких і повинні створюватись системи безпеки.

На сьогодні відповідних чітких критеріїв які б враховували особливості економічного та технічного розвитку регіону (держави, суспільства) не існує, що зі свого боку породжує питання об адекватності заходів з попередження та ліквідації до імовірних втрат в наслідок прогнозуємої аварії чи надзвичайної ситуації.

В якості критерію, який є базою для формування управлінського рішення стосовно комплектування тими чи іншими засобами попередження та протидії доцільно прийняти критерій СІБ – «ефективність – інтегральна ціна». Остання є функцією низки формуючих показників [63].

Формування відповідного базового критерію, який є основою для вибору технічних засобів інтегральної системи безпеки у запропонованому вигляді в змозі відповісти на ряд питань, а саме: чи повинні втрати на безпеку ОЗ сягати щорічно запропонованих відсотків (ψ) від прибутку; чи достатньо цієї суми для отримання необхідного рівня безпеки, чи навпаки забагато; який повинен бути термін такого фінансування; чи можливо нерівномірне фінансування СІБ (наприклад, на початковому етапі впровадити більше фінансування на створення системи безпеки, а потім зменшити обсяг фінансування для підтримки та її оновлення); як розподілити розміри фінансування між складовими системи інтегральної

безпеки (рис. 1.2); чому слід більше приділити уваги – організаційним заходам або технічним засобам (рис. 1.3); як вибрати із всього різноманіття технічних засобів представлених на ринку необхідне та інші питання.

Як вже зазначалося система інтегральної безпеки за функціональними признаками є багатокомпонентною системою (рис. 1.2). У зв'язку з цим, сума затрат на розбудову такої системи S^{CB} має вигляд:

$$S^{CB} \geq \frac{U}{k_U}; \quad 0 < k_U \leq \psi \quad [64, 65]; \quad (1.13)$$

$$S^{CB} = \sum_i S^{(i)},$$

де U – втрати, що прогнозуються; k_U – коефіцієнт не припустимості втрат; $S^{(i)}$ – витрати на i -ту складову інтегрованої системи безпеки; i – кількість складових.

Надалі слід ввести наступне припущення: з подальшого розгляду S^{CB} виключена цінова складова послуг по проведенню відповідних засобів на ринок. Вона приймається однаковою для усіх типів технічних засобів, оскільки її природа визначається складовими (бренд фірми, час знаходження останньої на ринку, політикою маркетингу та інше), які не впливають на об'єктивні показники ефективності технічних засобів і відповідно не змінюють природи формування запропонованого критерію. Це припущення справедливе у разі розгляду достатньо великою кількістю однотипних за своїм функціональним призначенням технічних засобів або їх структурних елементів.

Елементи які складають кожний компонент системи безпеки укрупнено можливо віднести до однієї з двох взаємовпливних практичних реалізацій, а саме: попередження виникнення прояв небезпеки або безпосередня ліквідація небезпеки (рис. 1.3). Дані напрямки реалізації поєднують організаційно-управлінські, профілактичні, оперативно-тактичні заходи та інженерно-технічних засоби.

Неможливість побудови універсальної системи безпеки та визначена цим необхідність розробки системи безпеки для кожного типу об'єкту ставить перед спеціалістами завдання про визначення пріоритетів розвитку цих складових, і відповідно завдання по розподілу обмеженого (1.13) економічного потенціалу.

Таким чином, затрати на реалізацію і-го елемента СІБ визначаються як:

$$S^{(i)} = S_{\text{попередж.}}^{(i)} + S_{\text{ліквідац.}}^{(i)}, \quad (1.14)$$

де $S_{\text{попередж.}}^{(i)}$ – затрати з попередження і-ої небезпеки; $S_{\text{ліквідац.}}^{(i)}$ – затрати з ліквідацію і-ої небезпеки.

Таблиця 1.2 – Вагомість складових системи безпеки у розподілі економічного потенціалу

Економічний потенціал		Система безпеки
1.	$S_{\text{попередж.}} \gg S_{\text{ліквідац.}}$	орієнтована на попередження небезпек
1.1	$(S_{\text{попередж.орг.}} + S_{\text{попередж.проф.}}) \gg S_{\text{попередж.техн.}}$	орієнтована на попередження небезпек, де домінує соціально-психологічної складова безпеки
1.1.1	$(S_{\text{попередж.орг.}} \uparrow + S_{\text{попередж.проф.}} \downarrow) \gg S_{\text{попередж.техн.}}$	
1.1.2	$(S_{\text{попередж.орг.}} \downarrow + S_{\text{попередж.проф.}} \uparrow) \gg S_{\text{попередж.техн.}}$	
1.2	$(S_{\text{попередж.орг.}} + S_{\text{попередж.проф.}}) \ll S_{\text{попередж.техн.}}$	орієнтована на попередження небезпек, де домінує інженерно-технічна складова безпеки
2.	$S_{\text{попередж.}} \ll S_{\text{ліквідац.}}$	орієнтована на ліквідацію небезпек
2.1	$(S_{\text{ліквідац.орг.}} + S_{\text{ліквідац.опер.-такт.}}) \gg S_{\text{ліквідац.техн.}}$	орієнтована на ліквідацію небезпек, де домінує соціально-психологічної складова безпеки
2.1.1	$(S_{\text{ліквідац.орг.}} \uparrow + S_{\text{ліквідац.опер.-такт.}} \downarrow) \gg S_{\text{ліквідац.техн.}}$	
2.1.2	$(S_{\text{ліквідац.орг.}} \downarrow + S_{\text{ліквідац.опер.-такт.}} \uparrow) \gg S_{\text{ліквідац.техн.}}$	
2.2	$(S_{\text{ліквідац.орг.}} + S_{\text{ліквідац.опер.-такт.}}) \ll S_{\text{ліквідац.техн.}}$	орієнтована на ліквідацію небезпек, де домінує інженерно-технічна складова безпеки
3.	$S_{\text{попередж.}} \approx S_{\text{ліквідац.}}$	рівно зорієнтована
3.1	п. 1.1 та п. 2.1	
3.2	п. 1.1 та п. 2.2	
3.3	п. 1.2 та п. 2.1	
3.4	п. 1.2 та п. 2.2	

Відповідно, затрати з попередження і-ої небезпеки (рис. 1.3) визначаються

як:

$$S_{\text{попередж.}}^{(i)} = S_{\text{попередж.орг.}}^{(i)} + S_{\text{попередж.проф.}}^{(i)} + S_{\text{попередж.техн.}}^{(i)}, \quad (1.15)$$

де $S_{\text{попередж.орг.}}^{(i)}$, $S_{\text{попередж.проф.}}^{(i)}$ та $S_{\text{попередж.техн.}}^{(i)}$ – затрати на організаційно-управлінські заходи, профілактичні заходи та технічні засоби з попередження і-ої небезпеки.

Затрати з ліквідації і-ої небезпеки визначаються як:

$$S_{\text{ліквідац.}}^{(i)} = S_{\text{ліквідац.орг.}}^{(i)} + S_{\text{ліквідац.опер.-такт.}}^{(i)} + S_{\text{ліквідац.техн.}}^{(i)}; \quad (1.16)$$

де $S_{\text{ліквідац.орг.}}^{(i)}$, $S_{\text{ліквідац.опер.-такт.}}^{(i)}$ та $S_{\text{ліквідац.техн.}}^{(i)}$ – затрати на організаційно-управлінські заходи, оперативно-тактичні заходи та технічні засоби з ліквідації і-ої небезпеки.

В залежності від характеристик ОЗ, наявності небезпек, їх природи та інших складових визначаються пріоритети щодо розбудови загальної спрямованості складових СІБ, що з свого боку визначає вагомість внеску відповідних складових (1.13) – (1.16) – табл. 1.2.

2. ЗАСТОСУВАННЯ КОНЦЕПЦІЇ ІНТЕГРАЛЬНОЇ БЕЗПЕКИ

2.1. Застосування концепції інтегральної безпеки для оцінки стану регіонів України (на прикладі «небезпека від надзвичайних ситуацій техногенного та природного характеру»)

Застосування формул розділу 1.3 до офіційно оприлюдненої інформації щодо стану об'єктів та росту внутрішнього валового продукту (ВВП), як базового показника стану системи [37, 50], дозволяє отримати наступні вирази (2.1, 2.2) та відповідно зміни якісної характеристики безпеки регіонів України за техно-

генною та природною складовою – рис. 2.1 – 2.5 (де $\Delta \text{ВВП}^m = \frac{\text{ВВП}_{m-1}}{\text{ВВП}_m}$ – характеристика зміни зростання внутрішнього валового продукту; ВВП_{m-1} – приріст ВВП у період (m-1); ВВП_m – приріст ВВП, який прогнозується у період m).

$${}^{(i)}k_m^{\text{техн.**}} = {}^{(i)}N_m^{\text{техн.*}} \frac{{}^{(i)}N_m^{\text{насел.*}}}{{}^{(i)}S_m^*} \quad (2.1)$$

$${}^{(i)}k_m^{\text{прир.**}} = {}^{(i)}N_m^{\text{прир.*}} \frac{{}^{(i)}N_m^{\text{насел.*}}}{{}^{(i)}S_m^*} \quad (2.2)$$

Таким чином, застосування базового принципу комплексної оцінки безпеки СІБ з урахуванням існуючого нормативно-правового, технічного та економічного потенціалу дозволяє визначити три рівні стану безпеки населення регіонів: $[0 \div 0.05]$ – стабільний; $[0.05 \div 0.1]$ – небезпечний (Луганська,

Харківська, Дніпропетровська та Львівська області); [більш 0.1] – особливо небезпечний (Донецька область), що у свою чергу підтверджується статистикою виникнення НС протягом 2007 – 2008 років.

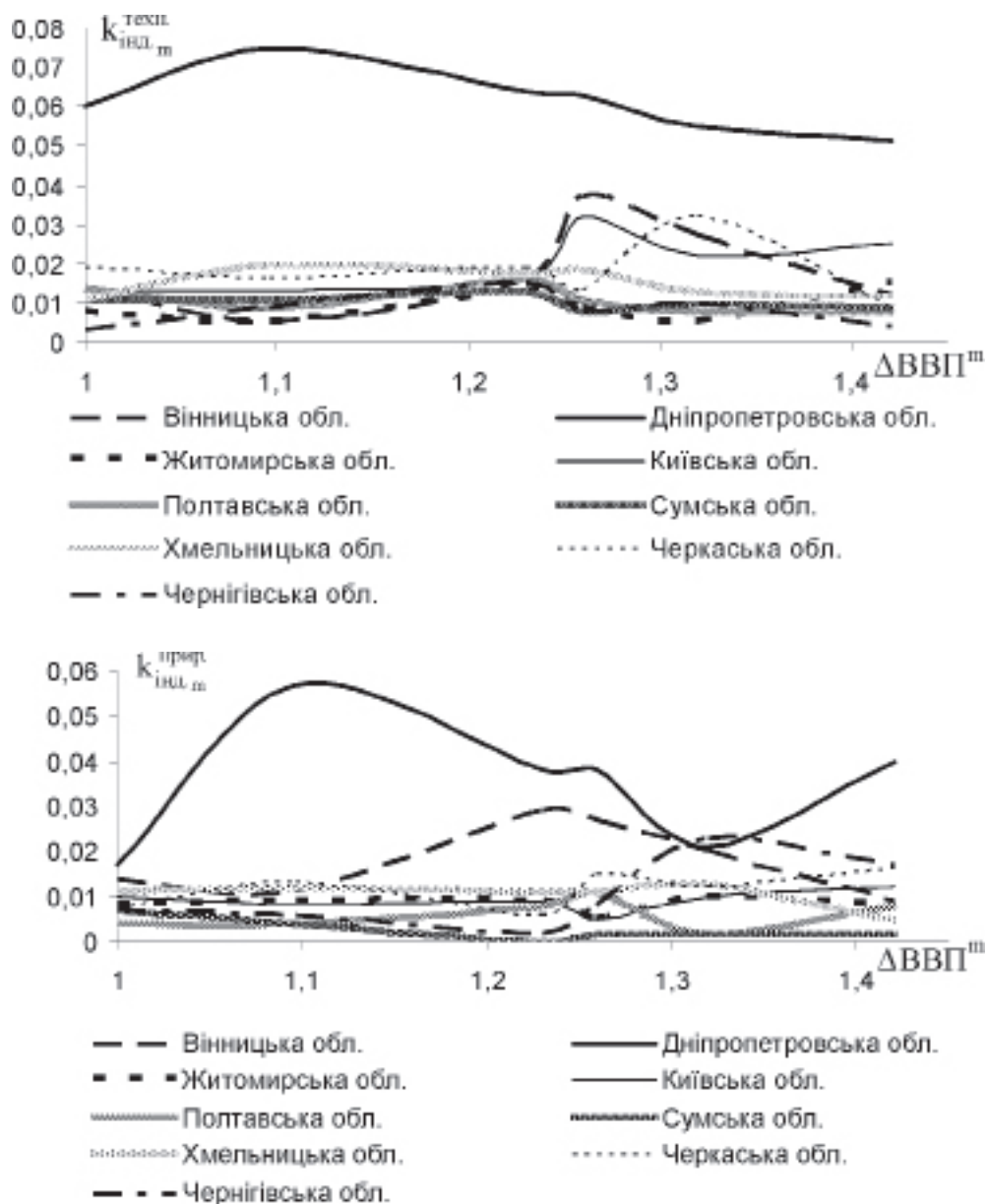


Рис. 2.1 – Динаміка зміни показника техногенної та природної небезпеки у центральних та північних регіонах України у відповідності до зміни $\Delta \text{ВВП}^m$ у 2003 -2007 рр.

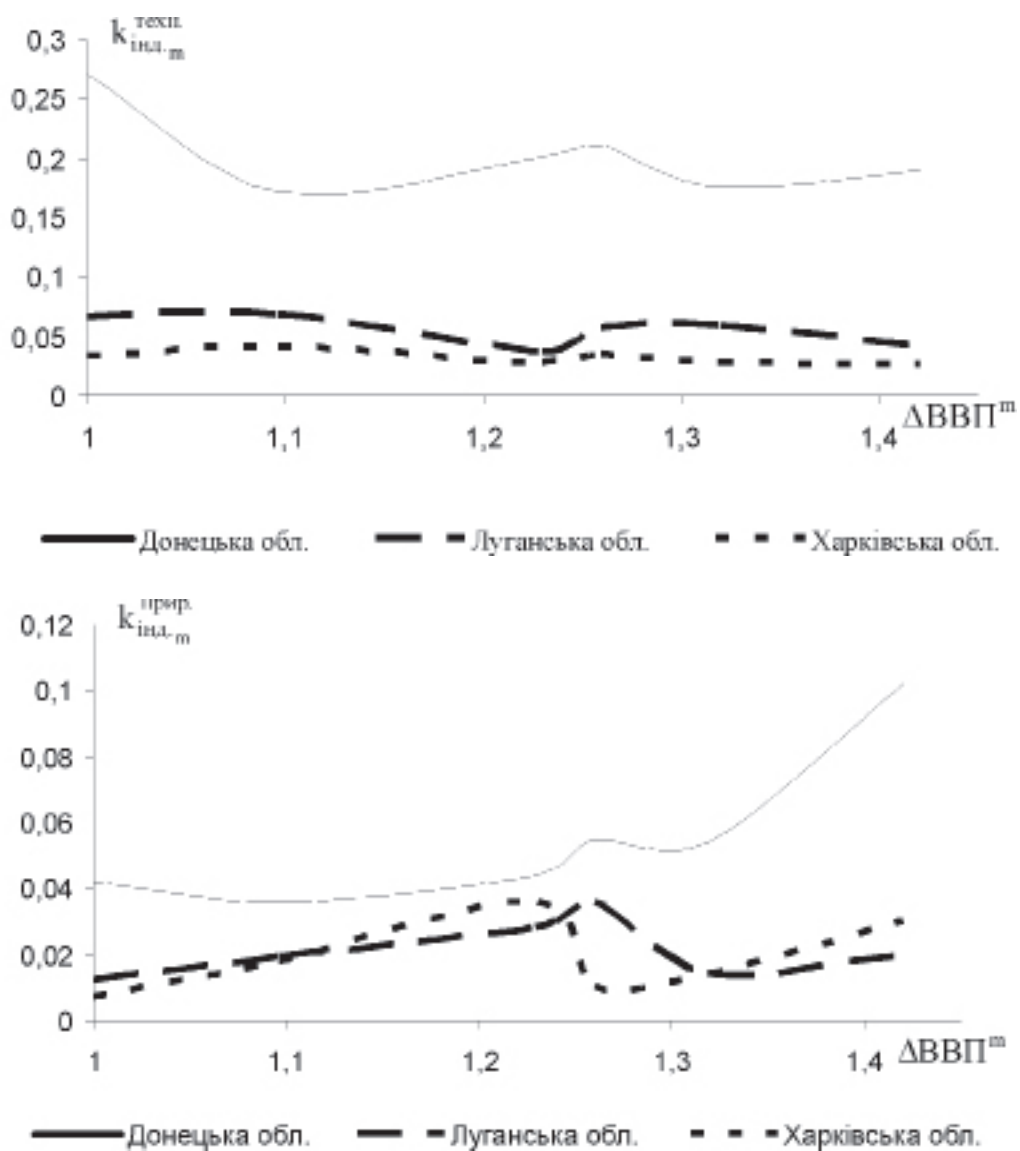


Рис. 2.2 – Динаміка зміни показника техногенної та природної небезпеки у східних регіонах України у відповідності до зміни $\Delta\text{ВВП}^m$ у 2003-2007 рр.

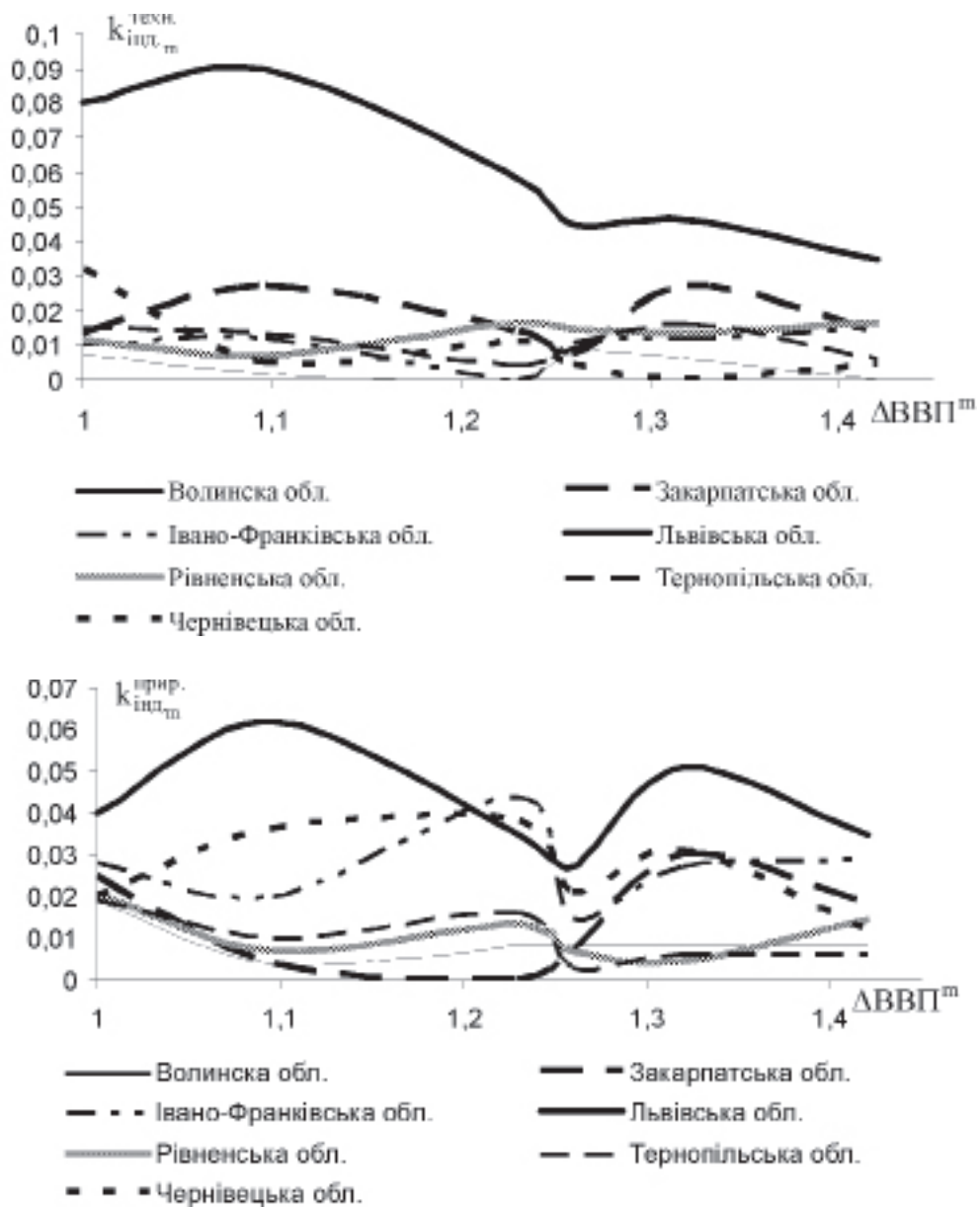


Рис. 2.3 – Динаміка зміни показника техногенної та природної небезпеки у західних регіонах України у відповідності до зміни $\Delta ВВП^m$ у 2003-2007 р.р.

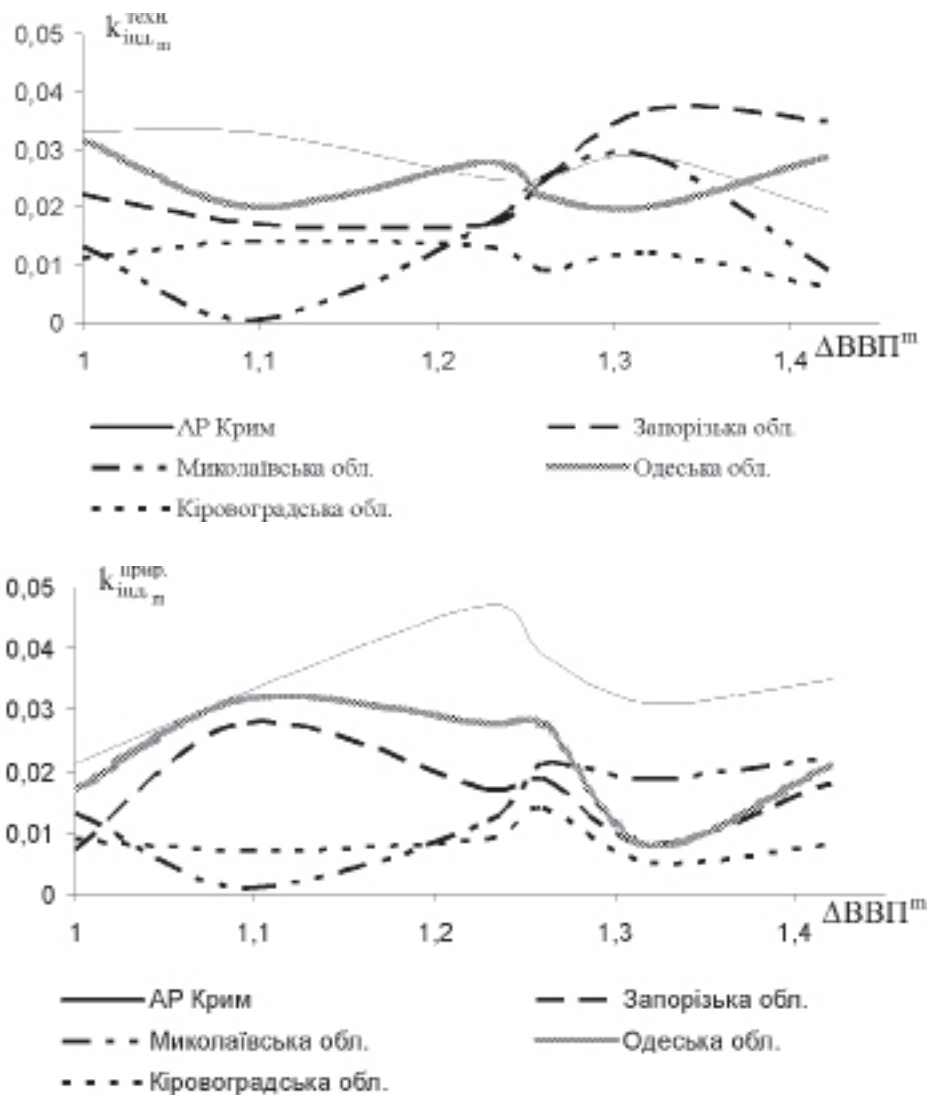


Рис. 2.4 – Динаміка зміни показника техногенної та природної небезпеки у південних регіонах України у відповідності до зміни $\Delta ВВП^m$ у 2003-2007 р.р.

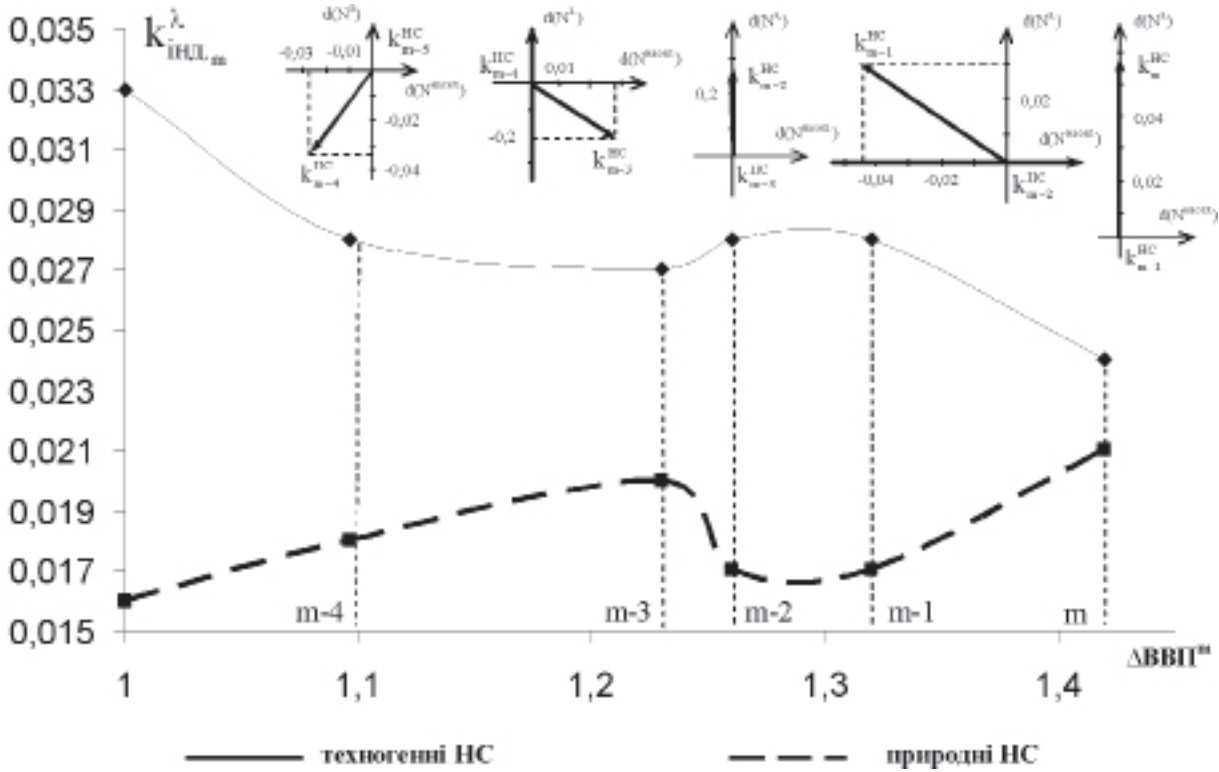


Рис. 2.5 – Динаміка зміни показника техногенної та природної безпеки в Україні у відповідності до зміни $\Delta \text{ВВП}^m$ у 2003-2007 р.р.

Аналізуючи динаміку зміни показника безпеки в цілому по Україні, у відповідності до зміни її економічного стану, слід визнати певну стабілізацію рівня безпеки населення України, незначні коливання, при умовах збільшення внутрішнього валового продукту, що обумовлено відсутністю ефективної стратегії розвитку національної безпеки держави [66] та створення відповідної системи безпеки. Покращення рівня безпеки в деяких регіонах відбувається лише за рахунок „зменшення” кількості населення у небезпечних зонах, що зможе опинитися під враженням небезпечних факторів НС.

Аналізуючи векторні діаграми напрямків покрокової зміни безпеки України у координатах „надзвичайні ситуації – населення” (рис. 3.5) слід наголосити на існування епізодичних сприятливих економічних умов розвитку безпеки України за період 2003 – 2007 р.р. на кроці (m-3), який обумовлений ростом кількості населення та зменшенням виникнення надзвичайних ситуацій.

Вкотре, слід наголосити на неможливість побудови універсальної для всіх регіонів системи безпеки та на необхідність територіально-диференційованого

підходу при розробці інтегрованої підсистеми безпеки функціонування природно-технічно-соціальної системи з територіально рознесеними параметрами – території України.

2.2. Застосування концепції інтегральної безпеки для оцінки стану регіонів України (на прикладі «хімічна небезпека»)

Безпека функціонування хімічно небезпечних об'єктів залежить від багатьох чинників: фізико-хімічних властивостей сировини, характеру технологічного процесу, конструкції та надійності обладнання, умов зберігання і транспортування хімічних речовин, стану контрольно-вимірювальних приладів та засобів автоматизації, ефективності засобів проти аварійного захисту, рівня організації профілактичної роботи, своєчасності і якості планово-запобіжних ремонтних робіт, підготовленості і практичних навичок персоналу, системи нагляду за станом технічних засобів проти аварійного захисту, тощо [67 – 69].

Офіційно існуюча система класифікації як адміністративно-територіальних одиниць регіонів, так і об'єктів господарчої діяльності, здійснюється за ступенем хімічної небезпеки, де єдиним показником виступає кількість населення, яка може опинитись (мешкає) у зоні можливого хімічного зараження [7, 8]. Ця оцінка є однокритеріальною, про що свідчать дані, наведені у табл. 2.1, і відповідно не може виступати об'єктивним критерієм класифікації об'єктів і території та відповідно прийматися у подальших розрахунках як ризику хімічних аварій та можливих збитків (загибель людей, матеріальні втрати), так і коштів та заходів (чисельність сил реагування, оснащення тощо), які повинні бути передбачені на їх ліквідацію.

Відповідно до оприлюдненої інформації [2 – 8] ступінь хімічної небезпеки в Україні (табл. 2.1) у порівнянні з 2002 та 2003 роками (II ступінь) зменшився до III ступеню у 2004 та 2007 роках та IV ступеню (найнижчого) у 2008 році, що, на наш погляд, зумовлено лише негативним демографічним фактором скороченням населення, яке постійно мешкає у зонах можливого хімічного зараження (міграція, процес урбанізації які офіційною методою також не враховуються).

Натомість, об'єктивні показники свідчать про досить складний (а в деяких регіонах навіть критичний) стан хімічної небезпеки, завдяки майже повній

зношеності обладнання, морально застарілим технологіям, відсутності ремонтної бази та виробництва комплектуючих деталей, відсутності науково обґрунтованих робіт у сфері побудови комплексних систем безпеки, які враховували б об'єктивний стан об'єктів та поведінку присутніх у технологічних процесах хімічно небезпечних речовин. Більш об'єктивним є поділ хімічно небезпечних об'єктів у відповідності до технології обертання хімічних речовин у виробничих процесах. За цією класифікацією всі об'єкти поділені на 59 категорій [23]. Утім і вона має ряд недоліків, а саме, детально розрізняючи об'єкти з виготовлення та переробки компонентів, що містять небезпечні хімічні сполуки, поєднує хвостосховища небезпечних хімічних речовин та продуктопроводи під загальною категорією „інші хімічно небезпечні об'єкти” і також не дозволяє об'єктивно оцінити рівень безпеки об'єктів і регіонів у яких вони розташовані.

Таблиця 2.1- Статистичні дані щодо стану хімічної небезпеки території України

Рік	Загальний ступінь хімічної небезпеки	Кількість хімічно небезпечних	Кількість хімічно небезпечних об'єктів	Кількість НХР (тис. тон)	Кількість населення у зоні можливого хімічного зараження (тис. чол.)	Наявність систем виявлення НХР
2002	II	276	1771	300,64	21243,65	579
2003	II	434	1575	293,9	17009,38	624
2004	III	403	1560	235,57	15890,42	609
2005	III	445	1572	332,6	13823,37	678
2006	III	392	1524	355,93	11984,07	651
2007	III	413	1488	314,27	11660,77	684
2008	IV	426	1414	356,49	10061,44	дані відсутні

Концепція інтегральної безпеки передбачає проведення аналізу хімічно небезпечного стану регіонів України та класифікацію адміністративно-територіальних одиниць регіонів України й відповідних об'єктів за динамікою (швидкість зростання або зменшення) прогнозованих негативних збитків. Цей показник, у разі збереження існуючої динаміки змін кількості та якості хімічно небезпечних об'єктів (стан обладнання); небезпечних хімічних речовин, що обертуються в їх технологічному процесі; населення; систем безпеки та контролю

за станом об'єктів та територій на яких вони розміщені; рівня професійної та психофізіологічної підготовки персоналу відповідних об'єктів, дозволить не тільки констатувати стан хімічної небезпеки, але й на далі спрогнозувати її зміни з метою дієвого перерозподілу існуючих матеріальних та людських резервів.

Враховуючи штучне обмеження існуючих на сьогодні даних щодо показників безпеки хімічно небезпечних об'єктів України 2007 ÷ 2008 років, доцільним є прогнозування на базі комбінованого методу [70], що поєднує прогнозування на підставі пропорційних залежностей та багатofакторного регресивного аналізу в частині визначення коефіцієнту зміни хімічно небезпечного стану регіонів.

В основі запропонованого методу містяться достатньо зрозумілі наступні припущення: по-перше, процеси виникнення аварій та надзвичайних ситуацій техногенного характеру на хімічно небезпечних об'єктах взаємопов'язані та, по-друге, мають певну інерційність. Останнє означає, що вага практичного будь-якого показника в момент аналізу (m) залежить відповідним чином від його минулого стану в моменти ($m-1, \dots m-n$).

Якщо ці припущення розповсюдити безпосередньо на конкретні об'єкти групи, що вивчається, слід зазначити, що ОЗ, у нашому випадку потенційно хімічно небезпечний об'єкт, це діюча система узгоджених окремих елементів (як якісно, так і кількісно вимірюваних). Це значить, що багато показників, які не пов'язані між собою формалізованими залежностями, між тим змінюються в динамічній узгодженості. Відповідно, якщо наведена система знаходиться у стані рівноваги, то окремі її елементи не в змозі діяти хаотично, у разі варіабельність дій має певні обмеження. Відповідно інерційність, у контексті окремого об'єкту, матиме сенс лише на стабільно працюючому ОЗ (підприємстві) при визначенні загальних показників системи безпеки [55, 71 – 73]. На безпосередню поведінку факторів, які можуть призвести до аварійної ситуацій, окрім їх „історії”, вагомий вплив матимуть випадкові процеси пов'язані з технологією обертання небезпечних речовин, безвідмовністю систем моніторингу та контролю, психофізіологічні обставини, тощо [71 – 73].

Відповідно на макрорівні очікувані збитки $Y_{\text{прог}}^m$ дорівнюють:

$$Y_{\text{прог}}^m = Y_o^{m-1} * K_{\text{зхнс}}^m, \quad (2.3)$$

де Y_0^{m-1} – збитки за останній звітний період (m-1); $K_{\text{ЗХНС}}^m$ – коефіцієнт зміни хімічно-небезпечного стану у прогнозованому періоді (m), який визначається за формулою

$$K_{\text{ЗХНС}}^m = K_{\text{инф}}^m * \frac{K_{\text{вЛN}}^m * \Delta N^m * K_{\text{вЛQ}}^m * \Delta Q^m * K_{\text{вЛL}}^m * \Delta L^m * K_{\text{вЛП}}^m * \Delta \Pi^m * K_{\text{вЛB}}^m * \Delta B^m}{K_{\text{вЛSб}}^m * \Delta S_{\text{б}}^m} \quad (2.4)$$

В цьому виразі $K_{\text{инф}}^m$ – коефіцієнт очікуваної інфляції (знецінення) у m період; $K_{\text{вЛN}}^m = \frac{1}{1 - J_{\text{обл}}}$ – коефіцієнт небезпечних властивостей технологічного обладнання у m період, а $J_{\text{обл}}$ – відсоток очікуваного зносу технологічного обладнання на хімічно небезпечних об'єктах у m період ($0 < J_{\text{обл}} < 1$);

$$K_{\text{вЛQ}}^m = \frac{\sum_{i=1}^{\phi} (4 - K_i^{\text{небез}}) * Q_i}{\sum_{i=1}^{\phi} Q_i} \text{ – коефіцієнт властивостей небезпечно хімічних речовин}$$

(НХР), які присутні у технологічному процесі, де $K_i^{\text{небез}}$ – клас безпеки та приймає значення від (1 ÷ 3) у відповідності до діючої класифікації [74, 75], Q_i

– кількість i-ї СДОР, що обертається у технологічному процесі; $K_{\text{вЛL}}^m = \frac{\rho_i^{\text{плот}}}{\rho^{\text{плот}}}$ –

коефіцієнт нерівномірності впливу небезпечних факторів хімічних аварій на населення, де $\rho_i^{\text{плот}}$ – значення щільності населення i-го регіону (території

об'єкту) до $\rho^{\text{плот}}$ – загальної щільності на даній території; $K_{\text{вЛП}}^m = \frac{1}{1 - \theta_{\text{пер}}}$ –

коефіцієнт психофізіологічної небезпеки, де $\theta_{\text{пер}}$ – відсоток аварій внаслідок

незадовільних організаційних дій та помилок персоналу ($0 < \theta_{\text{пер}} < 1$); $K_{\text{вЛВ}}^m = \frac{\rho_i^{\text{HC}}}{\rho^{\text{HC}}}$ –

коефіцієнт очікуваного небезпечного впливу зовнішніх факторів навколишнього середовища, де ρ_i^{HC} значення нестабільності природного середовища i -го регіону

(території об'єкту) до ρ^{HC} загального стану виникнення природних надзвичайних

ситуацій на даній території; $K_{\text{вЛСб}}^m = \frac{1}{1 - \theta_{\text{Сб}}}$ – коефіцієнт небезпеки пов'язаної з

відмовами систем моніторингу та контролю за хімічно небезпечним станом об'єктів у m період, а $\theta_{\text{Сб}}$ – відсоток очікуваних відмов систем контролю та

безпеки хімічно небезпечних об'єктів у m період ($0 < \theta_{\text{Сб}} < 1$); $\Delta N^m = \frac{N_{m-1}}{N_m}$ –

характеристика зміни кількості хімічно небезпечних об'єктів, де N_{m-1} – кількість існуючих об'єктів у період $(m-1)$, N_m – кількість об'єктів, яка прогнозується у

період m ; $\Delta Q^m = \frac{Q_{m-1}}{Q_m}$ – характеристика зміни кількості небезпечних хімічних

речовин, що обертаються в технологічному процесі об'єктів, де Q_{m-1} – кількість існуючих НХР у період $(m-1)$, Q_m – кількість НХР, яка прогнозується у період m ;

$\Delta L^m = \frac{L_{m-1}}{L_m}$ – характеристика зміни кількості населення, яка мешкає на території

можливих зон хімічного враження від небезпечних хімічних ОЗ, де L_{m-1} –

кількість населення у період $(m-1)$, L_m – кількість населення, яка прогнозується

у період m ; $\Delta\Pi^m = \frac{\Pi_{m-1}}{\Pi_m}$ – характеристика зміни кількості обслуговуючого пер-

соналу на ОЗ, де Π_{m-1} – кількість персоналу у період $(m-1)$, Π_m – кількість пер-

соналу, яка прогнозується у період m ; $\Delta B^m = \frac{B_{m-1}}{B_m}$ – характеристика зміни

кількості надзвичайних ситуацій природного характеру, де B_{m-1} – кількість над-

звичайних ситуацій природного характеру в період $(m-1)$, B_m – кількість надзви-

чайних ситуацій природного характеру, яка прогнозується у період m ;

$\Delta S_6^m = \frac{S_{6m-1}}{S_{6m}}$ – характеристика зміни кількості систем виявлення небезпечних

хімічних речовин, де S_{6m-1} – кількість систем виявлення небезпечних хімічних

речовин у період $(m-1)$, S_{6m} – кількість систем виявлення небезпечних хімічних

речовин, яка прогнозується у період m .

Окремо слід зупинитися при визначенні базового показника, який би характеризував поділ на періоди під час формування прогнозу. Так, існуюча на сьогодні методика [2 – 8], спирається на простий часовий поділ періодів прогнозу (рік, півріччя, квартал тощо). Цей показник не пов'язаний з показниками стану хімічної небезпеки регіонів, а є лише констатацією періодів проведення вимірів (збору та отримання інформації). Більш детальний аналіз довів, що за базовий показник доречно вибрати один з наступних: зростання внутрішнього валового продукту (країни, регіонів); фінансування, яке виділяється на утримання об'єктів захисту; на рівні ОЗ, це кошти, які вкладаються у забезпечення ефективного функціонування СІБ ОЗ (модернізацію виробництва, моніторингу та контролю, підготовки персоналу тощо).

У результаті застосування наведених формул та на підставі офіційно оприлюдненої інформації щодо росту ВВП отримані результати щодо зміни якісної характеристики хімічно небезпечного стану регіонів України, що наведено в табл. 2.2.

Таблиця 2.2 - Динаміка змін кількісних характеристик хімічно небезпечного стану України

Рік	Базовий показник $\Delta\text{ВВП}^m$	ΔN^m	ΔQ^m	ΔL^m	ΔS_6^m	$K_{\text{ЗХНС}}^m$
2003	1,096	0,889	0,997	0,8	1,092	3,53
2004	1,23	0,99	0,801	0,934	0,975	4,52
2005	1,26	1,01	1,411	0,869	1,113	6,16
2006	1,32	0,97	1,07	0,867	0,96	5,44
2007	1,42	0,98	0,88	0,973	1,05	4,48
прогноз на 2008	1,5	1,02	1,01	1	1	5,85

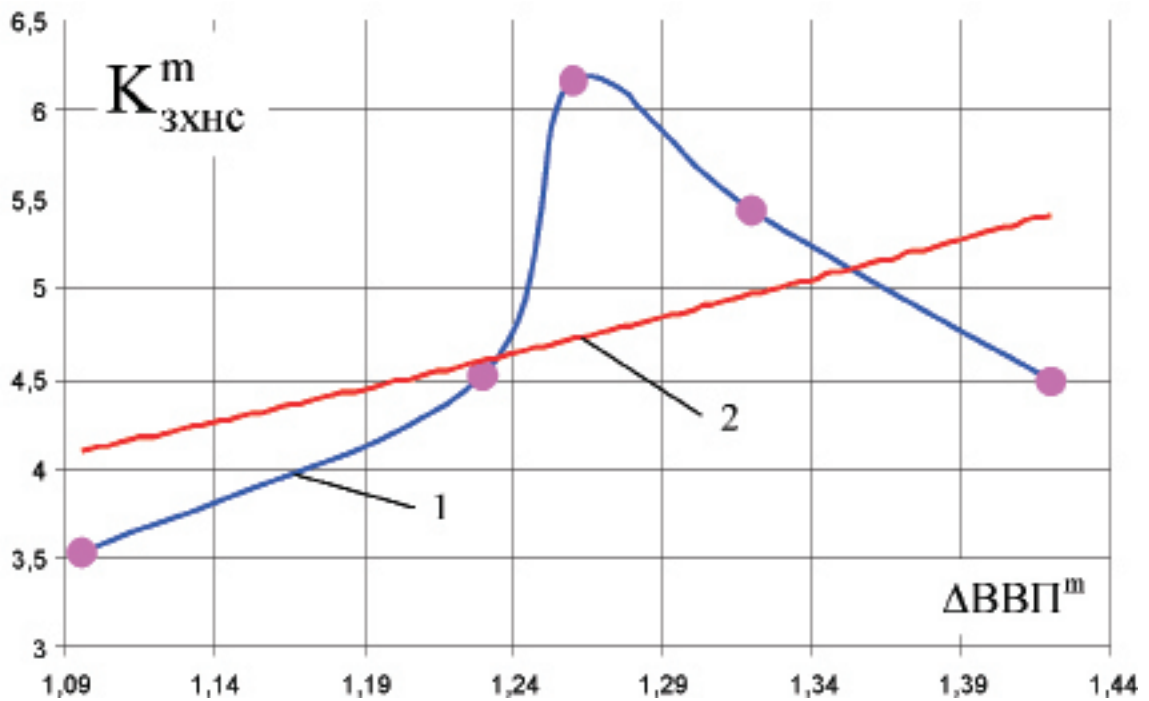


Рис. 2.6 – Динаміка зміни $K_{\text{ЗХНС}}^m$ у відповідності до зміни $\Delta\text{ВВП}^m$ у 2003-2007 рр.:
 1 – динаміка зміни $K_{\text{ЗХНС}}^m$; 2 – лінія тренду $K_{\text{ЗХНС}}^m$.

Побудова лінії тренду $K_{\text{ЗХНС}}^m$ (рис. 2.6) свідчить про стійке погіршення стану хімічної небезпеки України та недостатність заходів щодо поліпшення ситуації.

Відповідно були проведені розрахунки для кожного регіону України, які приведені у таблиці 2.3.

Показник ΔV^m має дещо іншу природу та потребує окремих додаткових

досліджень, тому на попередньому етапі його можна покласти рівним одиниці. Відповідно, отриманий прогноз коефіцієнту зміни хімічно небезпечного стану враховує лише фактори технічної природи.

Таблиця 2.3 – Прогноз динаміки змін кількісних характеристик хімічно небезпечного стану та коефіцієнтів впливу по регіонам України у 2008 році

Регіон	$K_{\text{влN}}^m$	ΔN^m	$K_{\text{влQ}}^m$	ΔQ^m	$K_{\text{влL}}^m$	ΔL^m	$\Delta S_{\text{б}}^m$	$K_{\text{зхнс}}^m$
АР Крим	4,35	0,9	1,97	4	0,99	0,3	0,95	11,47
Вінницька	3,11	1,05	1,82	3,05	0,84	1,1	0,2	99,97
Волинська	4,37	1	1,96	0,76	0,63	0,84	0,75	5,49
Дніпропетровська	1,6	1,33	1,87	1,29	1,41	1,32	1,03	11,08
Донецька	3,04	1,02	1,94	0,99	2,28	1,05	0,89	19,15
Житомирська	2,39	1	1,75	1,85	0,59	1,1	0,65	9,13
Закарпатська	3,82	0,75	1,9	1,6	1,22	0,5	0,7	9,07
Запорізька	2,26	1	1,65	1	0,9	1	1	3,99
Івано-Франківська	1,15	1	1,64	2,45	1,28	0,85	3,4	1,75
Київська	1,32	0,9	1,81	1,4	0,79	2,2	1	6,26
Кіровоградська	1,56	0,85	1,7	0,7	0,59	1,2	0,85	1,55
Луганська	2,33	1	1,93	0,5	1,21	1	1,1	2,95
Львівська	1,16	1,3	1,82	4	1,52	1,2	1,2	19,88
Миколаївська	3,78	1,05	1,9	0,9	0,65	2,25	0,75	15,7
Одеська	4,69	1,1	2	1,1	0,91	0,1	0,7	1,76
Полтавська	1,37	1	1,82	0,7	0,71	1,25	0,8	2,3
Рівненська	3,42	0,8	1,97	0,4	0,72	0,8	2,2	0,67
Сумська	1,49	1	1,87	0,85	0,68	0,75	1	3,37
Тернопільська	1,7	1,2	1,79	2,5	1,02	1,1	2	6,12
Харківська	2,76	1,02	1,9	1,1	1,16	1,35	0,98	11,19
Херсонська	4,94	1,9	1,996	3	0,52	3	2	52,56
Хмельницька	2,64	1,1	1,896	1,25	0,87	0,8	1	5,68
Черкаська	4,13	0,9	1,98	1,15	0,84	0,9	1,4	5,45
Чернівецька	1,69	1,15	1,55	0,9	1,4	0,5	0,5	4,52
Чернігівська	1,76	0,8	1,8	1,05	0,49	0,55	0,87	0,98
м. Київ	1,91	0,7	1,67	1,3	0,79	1,6	0,76	5,33
м. Севастополь	2,63	1	1,74	1	0,99	0,95	1,2	4,25

Як свідчить аналіз результатів, слід очікувати існуючу кількість нетипових результатів („викидів”) прогнозованих даних [61]. Відповідно до цих даних проведемо процедуру попарного видалення даних з наступною підстановкою середнього значення (табл. 2.4)

Таблиця 2.4 – Значення кількісних характеристик хімічно небезпечного стану отриманих після процедури корегування даних прогнозу

Регіон	Дані прогнозу				Кориговані дані			
	ΔQ^m	ΔL^m	ΔS^m	$K_{зхнс}^m$	ΔQ^m	ΔL^m	ΔS^m	$K_{зхнс}^m$
Вінницька	3,05	1,1	0,2	99,97	1,1	-	-	36,06
І в а н о -								
Франківська	2,45	0,85	3,4	1,75	1,1	-	-	0,8
Львівська	4	1,2	1,2	19,88	1,1	-	-	5,47
Миколаївська	0,9	2,25	0,75	15,7	-	0,97	-	6,77
Херсонська	3	3	2	52,56	1,1	0,97	-	6,23

На підставі отриманих коефіцієнтів $K_{зхнс}^m$ проведена класифікація регіонів України стосовно хімічної небезпеки за наступним критерієм: IV ступінь (покращення) – очікуваний коефіцієнт $K_{зхнс}^{mi}$ знаходиться в інтервалі

$$(0 \leq K_{зхнс}^{mi} \leq \frac{K_{зхнс}^{m \text{ серед}}}{2}); \text{ III ступінь (стабільний) – в інтервалі } (\frac{K_{зхнс}^{m \text{ серед}}}{2} < K_{зхнс}^{mi} \leq K_{зхнс}^{m \text{ серед}})$$

; II ступінь (погіршення) – в інтервалі $(K_{зхнс}^{m \text{ серед}} < K_{зхнс}^{mi} \leq \frac{3 K_{зхнс}^{m \text{ серед}}}{2})$; I ступінь

(критичне погіршення) – в інтервалі $(\frac{3 K_{зхнс}^{m \text{ серед}}}{2} < K_{зхнс}^{mi})$. Відповідно до введеного критерію маємо наступну картину щодо стану хімічної небезпеки у 2008 році – рис. 1.7.

Таким чином, в Україні має місце постійне погіршення хімічно небезпечного стану регіонів. Різниця полягає лише у швидкості цих процесів, яка залежить, у першу чергу, від стану технологічного обладнання підприємств, кількості та рівня досконалості систем контролю та виявлення НХР як територіального, так об'єктового рівнів.

Найбільше занепокоєння викликають ті регіони, де в частині НХР переважає аміак (Харківська, Луганська, Донецька, Одеська, Дніпропетровська області). У першу чергу це стосується підприємств, де ця речовина використовується в аміачно-холодильних установках, понад 80% з яких знаходяться у незадовільному стані. Слід зазначити, що попри хімічної небезпеки, ці підприємства становлять значну пожежовибухонебезпеку. По-друге, зазначені регіони мають досить високу щільність населення, яке, внаслідок територіального розміщення хімічно

небезпечних об'єктів, переважно концентрується у зонах можливого хімічного зараження та у зонах ураження внаслідок можливих вибухів.

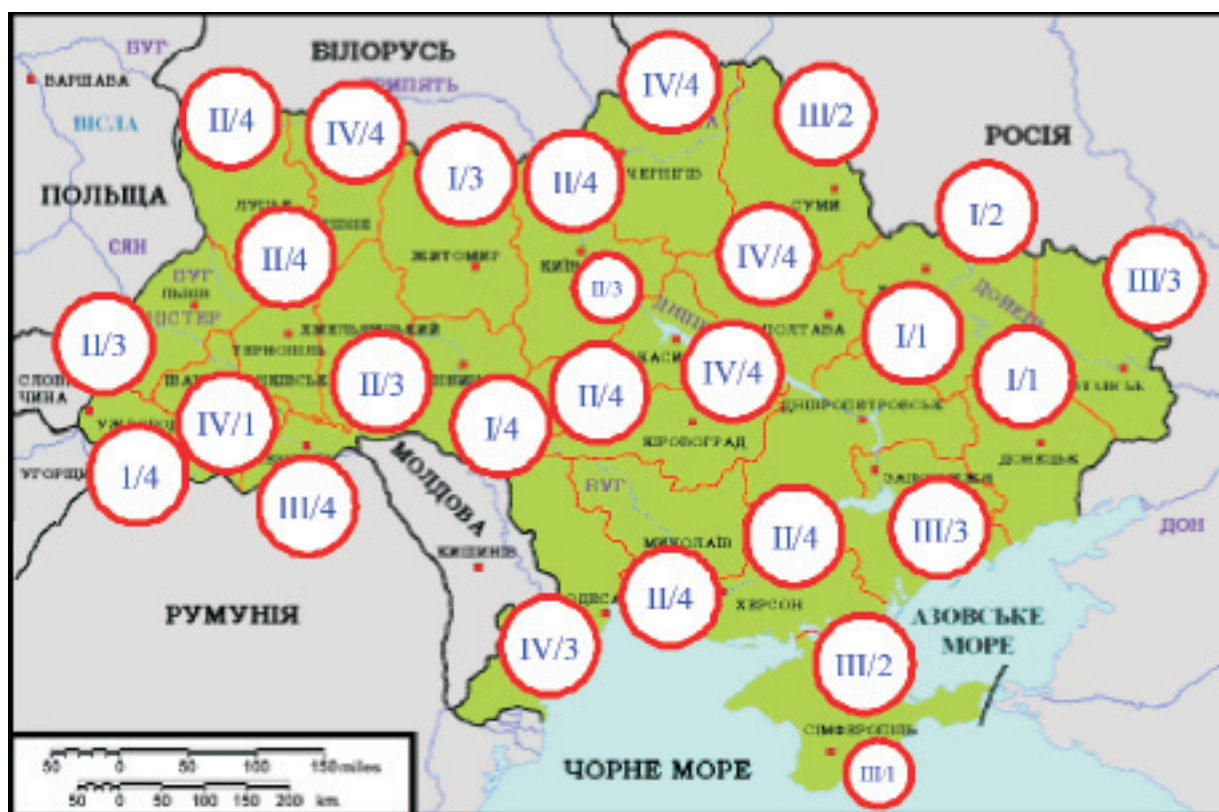


Рисунок 1.7 – Розподіл регіонів України за ступенем хімічної небезпеки (у чисельнику розподіл за прогностичним коефіцієнтом $K_{\text{зхнс}}^m$ на 2008р., у знаменнику за офіційною методикою [2 – 8])

До групи підвищеного ризику слід віднести і підприємства з нафтопереробки та регіони, де ці об'єкти становлять переважну більшість.

Постійно зростає небезпека, яку формують невеликі, з погляду наявності на них об'ємів НХР, об'єкти, що обумовлено: відсутністю на них дійових систем контролю та реагування на можливі аварії, розміщенням в густонаселених регіонах (як правило у містах), відсутністю чіткого нагляду з боку контролюючих органів, постійною зміною форми власності цих підприємств, високим рівнем залежності „малих” підприємств від негараздів політичного та соціального характеру і як наслідок відсутністю довгострокової політики по забезпеченню дієвої безпеки цих підприємств.

Запропонована модель прогнозу хімічно небезпечного стану регіонів

потребує постійного уточнення у процесі її використання та отримання відповідних статистичних даних. У той же час потребує перегляду відповідна звітність, яка на сьогодні здійснюється з регіонів до МНС України, та носить вибірковий та неточний характер (приклад 2008 р. [8]).

Застосування запропонованого підходу до визначення стану безпосередньо хімічно небезпечних об'єктів можливо лише для апріорної оцінки та потребує подальших досліджень щодо визначення природи факторів існуючої небезпеки та механізмів їх впливу на загальну безпеку об'єкту захисту.

2.3. Застосування концепції інтегральної безпеки для оцінки безпеки функціонування підприємства (на прикладі підприємств нафтопереробної промисловості)

Нафта та нафтопродукти є одним із значних за масштабом забруднення навколишнього природного середовища. В наслідок техногенних та аварійних розливів нафтопродуктів, утворення несанціонованих звалищ нафтовміщуючих промислових відходів виникають додаткові небезпечні фактори, які впливають на загальний рівень безпеки регіонів та створюють природоохоронні проблеми. Ґрунтам загрожує техногенне перетворення, майже зовсім подавляється життєдіяльність біоти, порушується фізико-хімічні та біологічні властивості навколишнього середовища.

Втрати нафти та нафтопродуктів під час видобутку, транспортування, переробки та збереження оцінюються мільйонами тонн щорічно [65, 66], при цьому збитки оцінюються мільярдами доларів. Близько половини цих випадків припадає на підприємства нафтопереробної промисловості (табл. 2.5), що свідчить про високу техногенну безпеку цих об'єктів.

У той же час, виходячи із існуючих на сьогодні економічних реалій, інвестування додаткових коштів на підвищення ефективності функціонування системи інтегральної безпеки за тим чи іншим небезпечним фактором повинно проводитись на основі всебічного експертного аналізу. Практичне застосування підходу викладеному у розділі 1.4 дозволило провести наступну процедуру та отримати відповідні результати.

Таблиця 2.5 – Розподіл великих збитків за видами діяльності

Діяльність	% від загального числа збитків	% від загальної суми збитків
Нафтопереробні заводи	46	35
Хімія/нафтохімія	32	28
Переробка газу	7	7,5
Термінали/резервуарні парки	7	3
Трубопроводи/насосні станції	1	0,5
Морські промисли	7	26

Таблиця 2.6 – Результати експертної оцінки факторів небезпеки нафтопереробного підприємства [51]

	Пожежі або вибухи в наслідок техногенних аварій	Аварії в наслідок помилок оператора	Аварії в наслідок пограбування шляхів транспортування	Аварії в наслідок терористичних дій	Екологічні аварії в наслідок природних катастроф	Аварії в наслідок
Експерт 1	0,3	0,4	0,2	0,05	0,025	0,025
Експерт 2	0,35	0,35	0,2	0,025	0,025	0,05
Експерт 3	0,4	0,2	0,25	0,05	0,075	0,025
Експерт 4	0,2	0,5	0,1	0,05	0,1	0,05
Експерт 5	0,25	0,4	0,2	0,1	0,025	0,025
Експерт 6	0,35	0,25	0,2	0,1	0,075	0,025
Експерт 7	0,4	0,3	0,1	0,05	0,1	0,05
Експерт 8	0,15	0,4	0,25	0,05	0,1	0,05
Експерт 9	0,35	0,4	0,15	0,05	0,025	0,025
Експерт 10	0,25	0,4	0,2	0,025	0,1	0,025
Експерт 11	0,3	0,45	0,15	0,05	0,025	0,025
Експерт 12	0,3	0,4	0,2	0,05	0,025	0,025
Експерт 13	0,3	0,45	0,2	0,025	0,025	0
Експерт 14	0,25	0,45	0,2	0,05	0,025	0,025
Експерт 15	0,4	0,4	0,05	0,05	0,05	0,05
Експерт 16	0,35	0,35	0,2	0,05	0,025	0,025
Експерт 17	0,35	0,4	0,15	0,05	0,025	0,025
Експерт 18	0,2	0,45	0,25	0,025	0,05	0,025
Експерт 19	0,25	0,45	0,1	0,05	0,1	0,05
Експерт 20	0,3	0,4	0,2	0,05	0,025	0,025
Експерт 21	0,3	0,4	0,15	0,05	0,075	0,025
Експерт 22	0,35	0,35	0,2	0,05	0,025	0,025
Експерт 23	0,25	0,3	0,1	0,1	0,2	0,05
Експерт 24	0,25	0,25	0,1	0,1	0,25	0,05
Усереднена оцінка	0,298	0,379	0,171	0,054	0,066	0,032

Так в якості експертів на першому етапі було визначено шість фахівців у сфері протипожежного, екологічного та інформаційного захисту, а також фахівців

у сфері нафтопереробної промисловості. Цим фахівцям в свою чергу було запропоновано вибрати, також, по шість фахівців. Таким чином, було визначено 22 фахівця з урахуванням перших шести, прізвища яких не повторюються. Наступний етап відбору виявив лише двох нових фахівців, які у свою чергу нових фахівців не виявили. Відповідно, у проведенні експертної оцінки приймали участь 24 фахівця, яким були запропоновані наступні види потенційних небезпек нафтопереробного підприємства: пожежі або вибухи в наслідок техногенної аварії, аварії в наслідок помилок оператора; аварії внаслідок пограбування шляхів транспортування нафтопродуктів; аварії в наслідок терористичних дій, екологічні аварії внаслідок природних катастроф; аварії внаслідок інформаційного проникнення або несанкційного отримання інформації.

Далі у відповідності до наведеної методики були отримані усереднені оцінки впливу небезпек (табл. 2.6).

Як видно з табл. 2.6 найбільшу занепокоєність викликає підготовка та професійні дії операторів, в тому числі їх можливість щодо прийняття антикризових рішень в різних ситуаціях, а також фактор старіння технологічного обладнання, економічні негаразди. В той же час, відносна соціальна та природна стабільність регіону призвела до незначних показників за іншими напрямками.

2.4. Застосування концепції інтегральної безпеки для комплектування технічними засобами (на прикладі «пожежна безпека»)

Запропонований загальний підхід до визначення пріоритетів з техніко-економічного обґрунтування засобів системи безпеки (розділ 1.5) розглянемо на прикладі розбудови системи типу 1.2 – табл. 1.2. Відповідно маємо:

$$S_{\text{попередж.техн.}}^{(i)} = S_{\text{пт}_1}^{(i)} + S_{\text{пт}_2}^{(i)} + S_{\text{пт}_3}^{(i)}, \quad (2.5)$$

де $S_{\text{пт}_1}^{(i)}$ – складова ціни засобу попередження небезпеки, яка обумовлена вибором типу технічного засобу; $S_{\text{пт}_2}^{(i)}$ – складова ціни засобу попередження небезпеки, яка

обумовлена його технічними характеристиками (рис. 2.8); $S_{птр_3}^{(i)}$ – складова ціни засобу попередження небезпеки, яка обумовлена показником небезпеки ОЗ на якому даний засіб планується застосовувати.

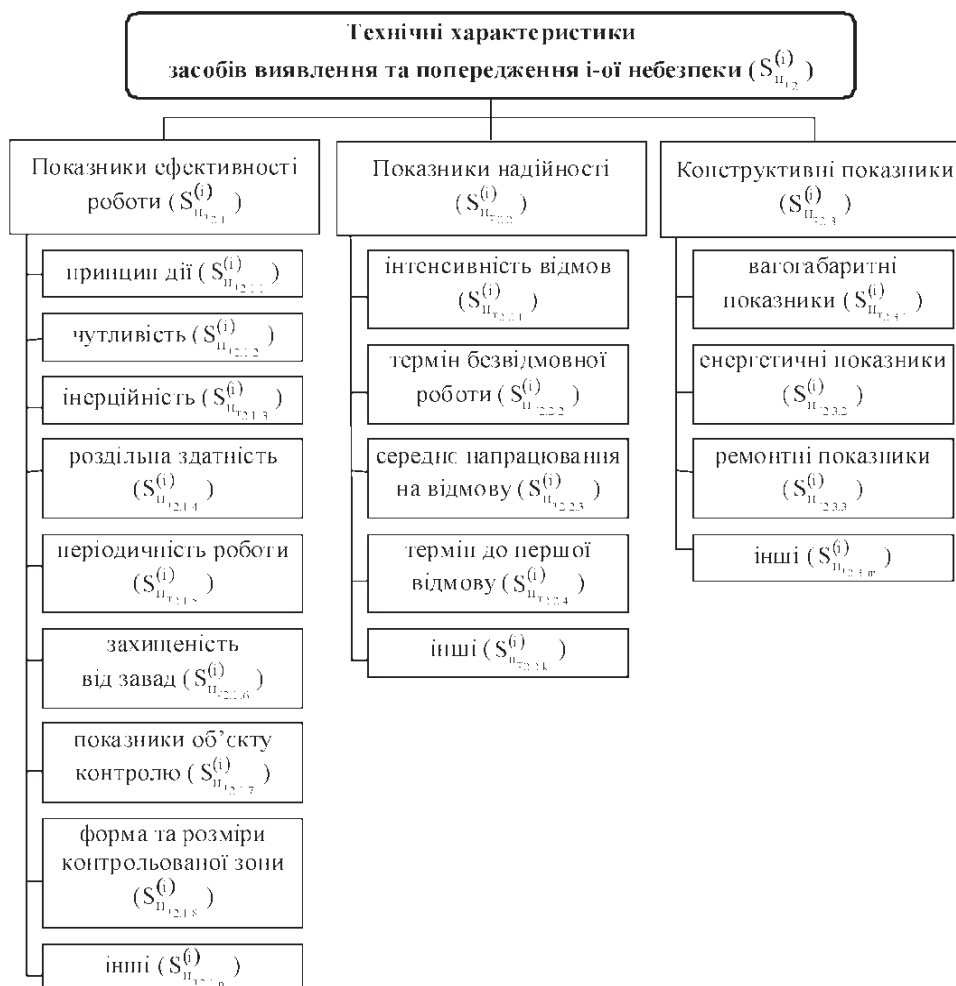


Рис. 2.8 – Загальний підхід до визначення показників технічних засобів виявлення та попередження небезпек

Застосування принципу комплектування технічними засобами за критерієм «ефективність – інтегральна ціна» до складової «пожежна безпека», дозволяє умовно класифікувати технічні засоби за функціональним призначенням у вигляді представленому на рис. 2.9 та рис. 2.10.

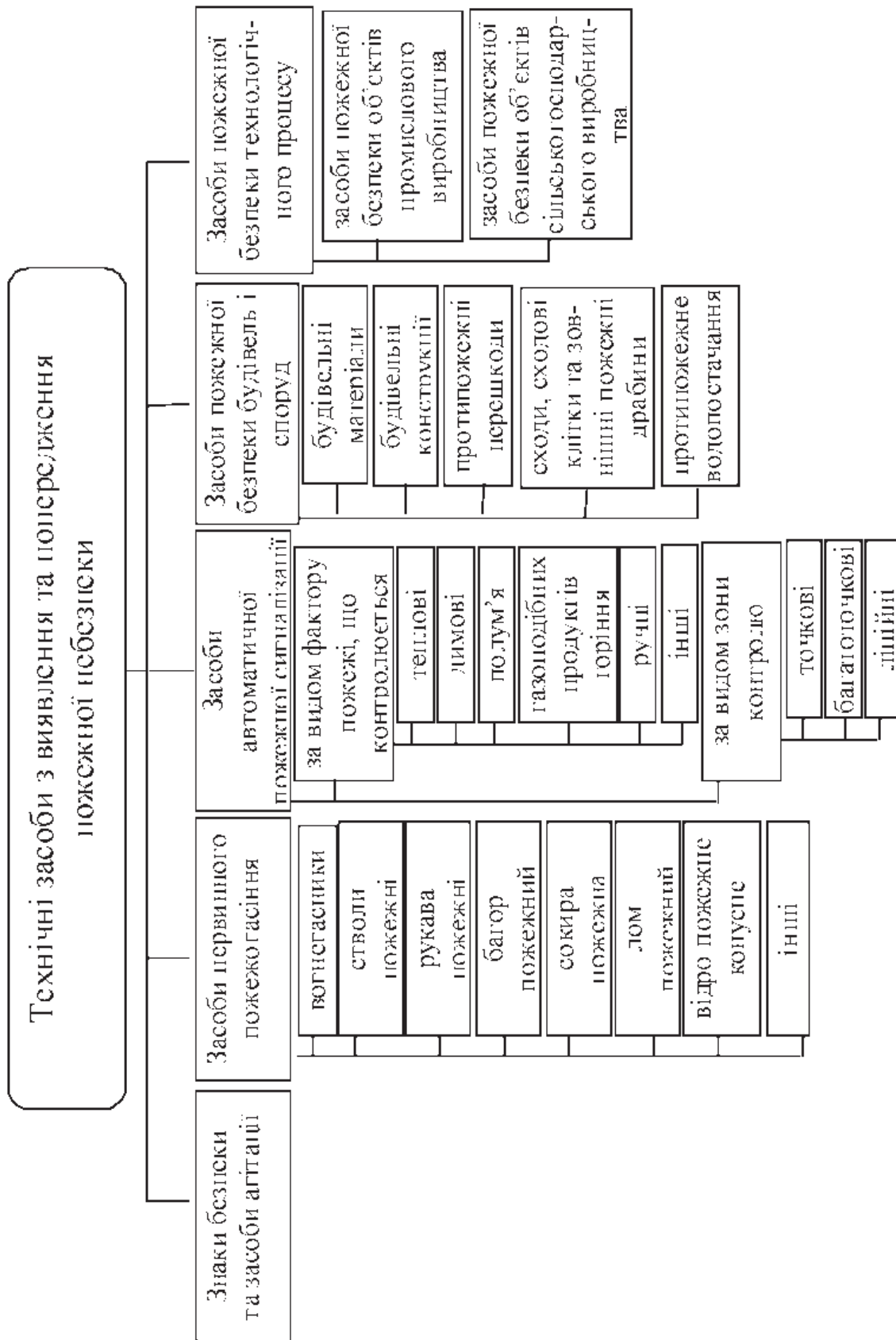


Рис. 2.9 – Структура технічних засобів з попередження пожежної небезпеки

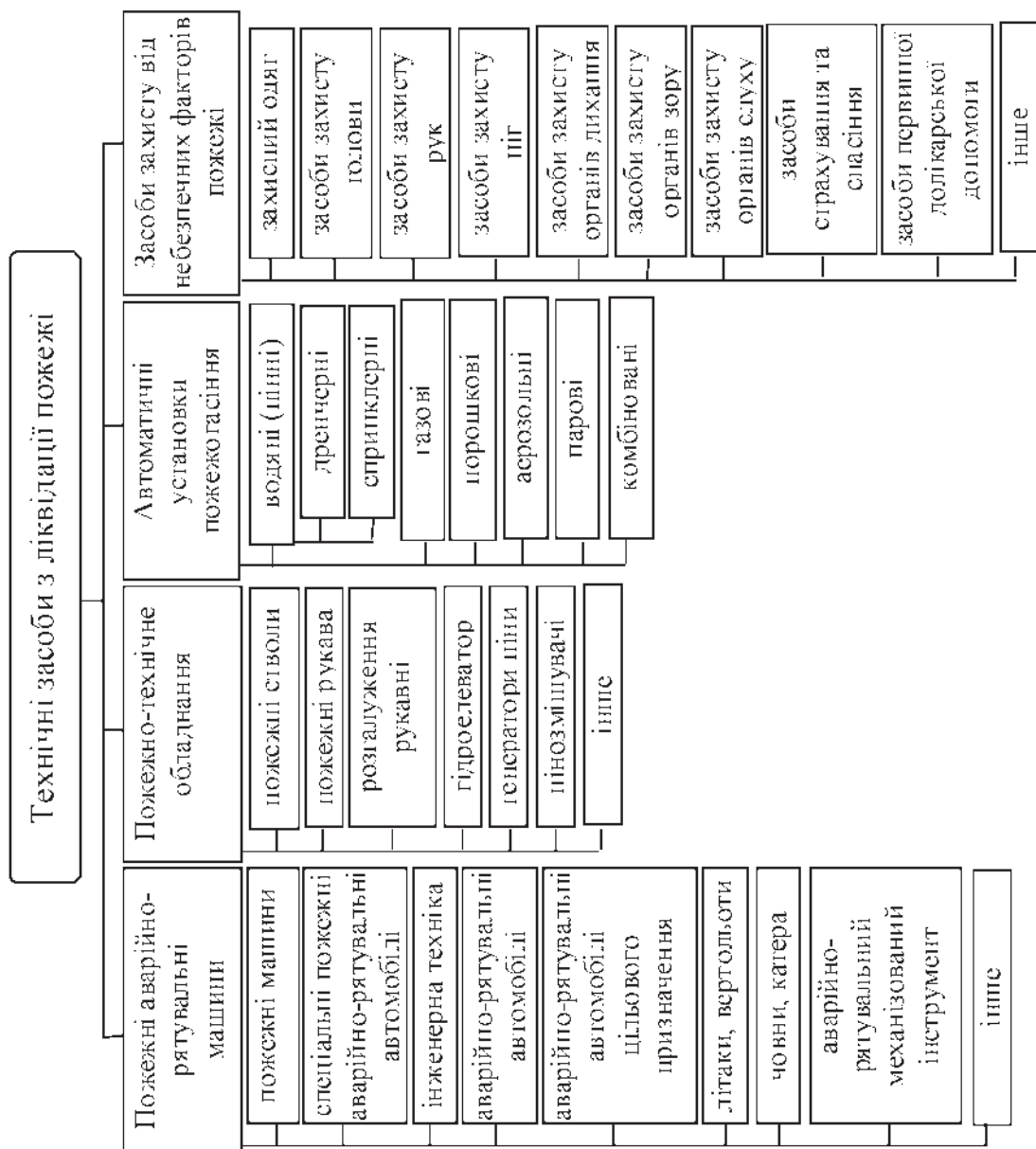


Рис. 2.10 – Структура технічних засобів з ліквідації пожежі

В межах складової «пожежна безпека» критерій було використано до розгляду засобів автоматичної пожежної сигналізації, що дало змогу підтвердити істинність раніше введених припущень та відповідність критерію. Використовуючи офіційно оприлюднені данні та інформацію відомих у даному напрямку виробників [76 – 99], за наведеним критерієм проведено аналіз засобів автоматичної пожежної сигналізації. Результати представлено у табл. 2.5 – табл. 2.10 та узагальнено на рис. 2.11.

Таблиця 2.5 – Характеристики теплових пожежних сповіщувачів (точкових)

Найменування приладу	Принцип дії приладу	Пріоритетна характеристика		Ціна	
		поріг виявлення, °C	швидкість збільш. темп., °C/хв.	кількісна, у.о.	якісна
ИП-103-5/3	макс. дії	80; 90; 100	–	0,47	$\bar{S}_{n_1}^{(i)}$
ИП-103-7	макс. дії	62		0,57	
ИП-103-5/1-А3 ИБ	макс. дії	70		0,89	
ИП-101-1А	макс. дії	70		2	
ИП 114-01-А1 Арго	макс. дії	58		3,91	
ИП-105-1D САУНА	макс. дії	99 – 115		5,18	
•••					
ИП 101-23-А1R (ЕСО1005)	макс.-діф. дії	58	8	11,39	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
ИП 101-31-А1R ПРОФИ-Т	макс.-діф. дії	58	8	18,48	
ИП 101-24А Leonardo-Т	макс.-діф. дії	58	8	26,04	
•••					
вибухобезпечне виконання					
ИП-101 ГРАНАТ	макс. дії	70; 90; 120	–	59,64	$S_{n_1}^{(i)} + \bar{S}_{n_3}^{(i)}$
ИП-103-2/1	–	70 ÷ 125		75,87	
•••					
5451EIS	макс.-діф. дії	58	8	92,4	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)} + \bar{S}_{n_3}^{(i)}$
•••					

Примітка: $S_{n_1}^{(i)}$ – базовий показник ціни; \bar{S}_{\dots} – домінуюча складова ціни.

Таблиця 2.6 – Характеристики димових пожежних сповіщувачів (точкових)

Найменування приладу	Принцип дії приладу	Пріоритетна характеристика (чутливість, дБ/м)	Ціна, у.о.	
			кількісна, у.о.	якісна
ИП-212-41М (ДИП-41М)	оптичний	0,05 ÷ 0,2	6,43	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
ИП 212-49 (ДИП-39)	оптичний	0,09 ÷ 0,144	7,93	
ИП-212-5СВ (ДИП-3СВ)	оптичний	0,05 ÷ 0,2	12,64	
ИП 212-73 ПРОФИ	оптичний	0,08 ÷ 0,16	19,8	
ПРОФИ-О (ИП 212-73)	оптичний	0,08 ÷ 0,16	20,02	
ДИП-34А	оптичний	0,05 ÷ 0,2	26	
ИП 212-60А LEONARDO-О	оптичний	0,08 ÷ 0,16	29,04	
• • •				
вибухобезпечне виконання				
1151EIS	радіоізотопний	–	125,4	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)} + \bar{S}_{n_3}^{(i)}$
• • •				

Таблиця 2.7 – Характеристики димових пожежних сповіщувачів (лінійних)

Найменування приладу	Принцип дії приладу	Пріоритетна характеристика (дальність дії, м)	Ціна, у.о.	
			кількісна, у.о.	якісна
ИПДЛ	оптичний	до 100	94,19	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
ИПДЛ-52 (ИП 212-52)	оптичний	8 ÷ 100	195,35	
СПЭК-2210	оптичний	10 ÷ 150	355,08	
• • •				

Таблиця 2.8 – Характеристики комбінованих пожежних сповіщувачів

Найменування приладу	Принцип дії приладу	Пріоритетні характеристики		Ціна, у.о.	
		поріг виявлення, °С	чутливість, дБ/м	кількісна, у.о.	якісна
ИП 212/101-4-А1R (ПРОФИ-ОТ)	комбінований	58	0,08 ÷ 0,16	22,04	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
ИП 212/101-3А (LEONARDO-ОТ)	комбінований	58	0,08 ÷ 0,16	35,64	
5192SDT	комбінований	57	–	83,58	
• • •					

Таблиця 2.9 – Характеристики пожежних сповіщувачів полум'я

Найменування приладу	Принцип дії приладу	Пріоритетні характеристики		Ціна, у.о.	
		чутливість, м	час спрацювання, сек	кількісна, у.о.	якісна
ПУЛЬСАР 1-01Н	виявлення ІЧ випромінювання	30	4,5	47,14	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
СПЕКТРОН-111С	принцип спектральної селекції	30	8	54,21	
ПУЛЬСАР 1-011С	виявлення ІЧ випромінювання	30	4,5	61,29	
СПЕКТРОН-123.С	виявлення ІЧ випромінювання	30	8	142,93	
• • •					
вибухобезпечне виконання					
СПЕКТРОН-123.Н	виявлення ІЧ випромінювання	30	8	128,14	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)} + \bar{S}_{n_3}^{(i)}$
ИП-332-1/1	принцип спектральної селекції	25	3	296,43	
• • •					

Таблиця 2.10 – Характеристики ручних пожежних сповіщувачів

Найменування приладу	Принцип дії приладу	Ціна, у.о.	
		кількісна, у.о.	якісна
ИПР-К	ручний пожежний сповіщувач з захисним склом	0,98	$\bar{S}_{n_1}^{(i)}$
ИР-1	ручний пожежний сповіщувач	5,08	
ИПР-3СУМ	ручний пожежний сповіщувач	6,02	
ИПР-Ксу	сповіщувач охорono-пожежний ручний	7,19	
ИПР	ручний пожежний сповіщувач	8,09	
ИПР-513-3А	ручний пожежний сповіщувач адресний	20,16	$S_{n_1}^{(i)} + \bar{S}_{n_2}^{(i)}$
• • •			

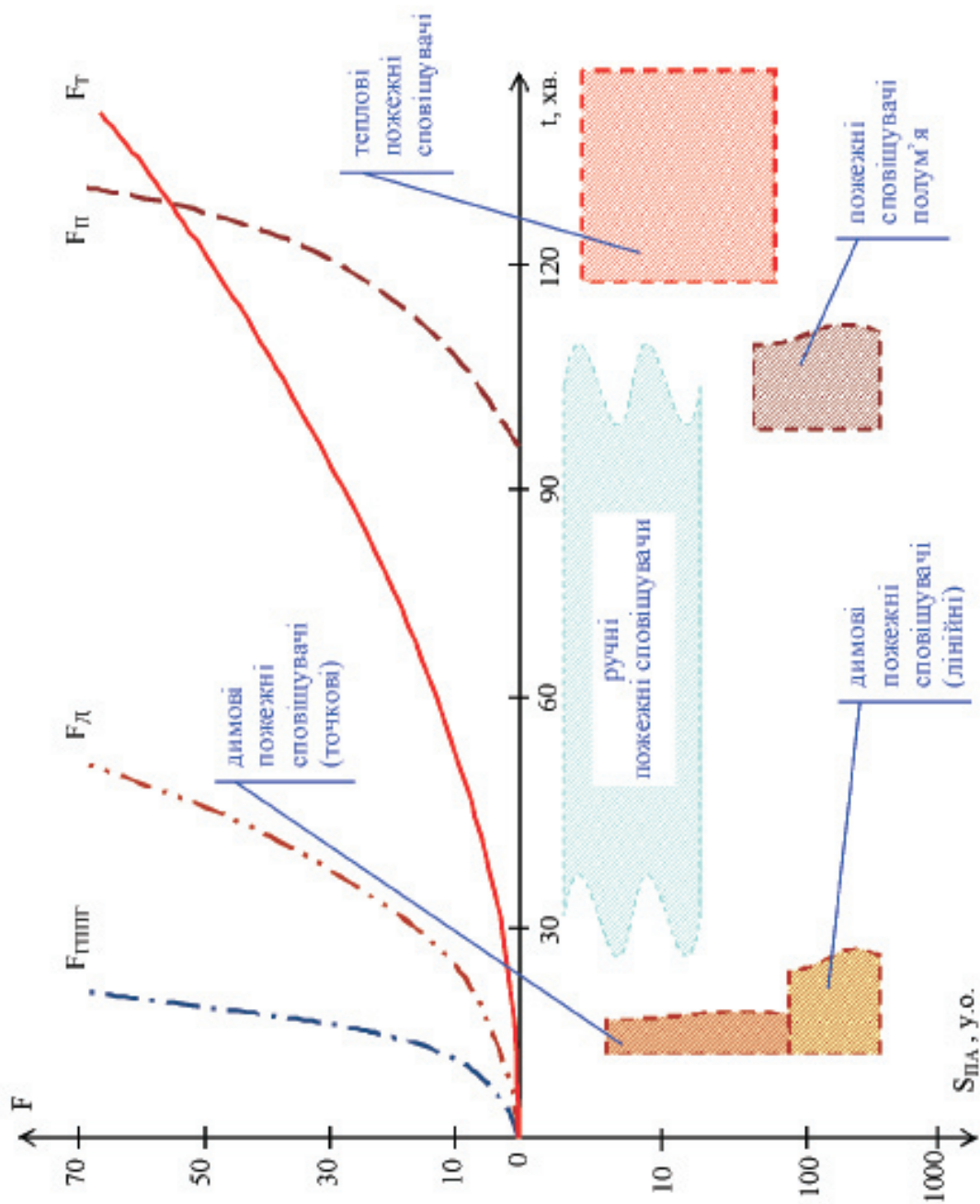


Рис. 2.11 – Графічне представлення областей функціонування технічних засобів автоматичної пожежної сигналізації в залежності від часу (t) прояви пріоритетних факторів небезпеки (F , де $F_{ГППГ}$ – газоподібні продукти горіння, $F_{Д}$ – дим, $F_{П}$ – полум'я, $F_{Г}$ – температура) [100], пріоритетних характеристик даних технічних засобів та їх інтегральної ціни ($S_{ПА}$)

Приклад безпосереднього вибору технічних засобів за сформованим критерієм наведено на рис. 2.12.

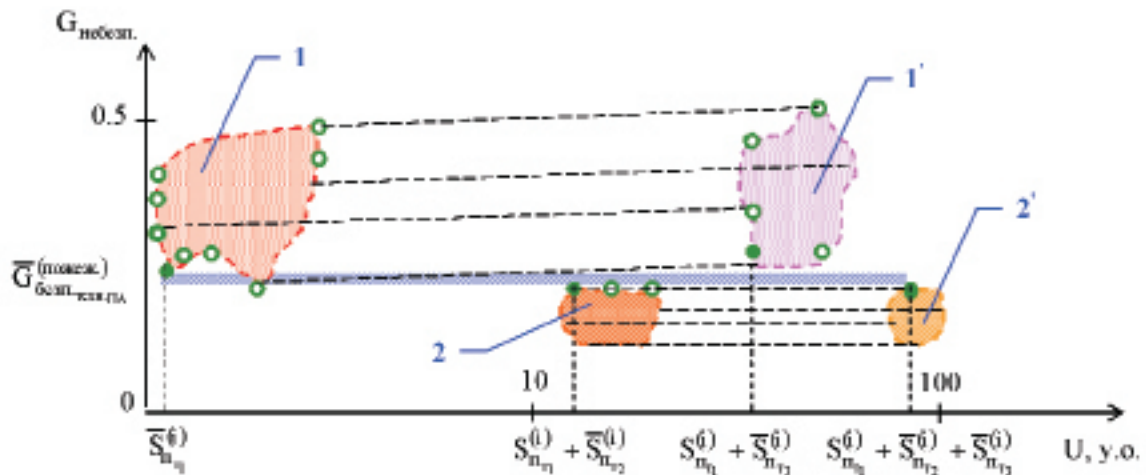


Рис. 2.12 – Залежність рівня пожежної безпеки від вибору точкових теплових пожежних сповіщувачів та затрат пов'язаних з профілактикою прояви пожежної небезпеки

($G_{\text{безп.техн.ПА}}^{(\text{пожеж.})}$ – середній рівень пожежної безпеки об'єкту контролю, який досягається за допомогою вибраного типу пожежного сповіщувача у системі пожежної автоматики; 1 – область вияву пожежі сповіщувачами максимальної дії; 1' – область вияву пожежі сповіщувачами максимальної дії у вибухобезпечному виконанні; 2 – область вияву пожежі сповіщувачами максимально-диференційної дії; 2' – область вияву пожежі сповіщувачами максимально-диференційної дії у вибухобезпечному виконанні)

2.5. Застосування концепції інтегральної безпеки для комплектування технічними засобами (на прикладі «інформаційна безпека»)

За даними досліджень проведеними Computer Security Institute та ФБР (CSI/FBI Computer Crime and Security Survey) розмір втрат від небезпеки у інформаційних системах розподілився наступним чином – рис. 2.13 [101].

Згідно рис. 2.13 найбільш небезпечними чинниками інформаційної безпеки виступають зовнішні впливання на інформації з метою її знищення або викривлення, а також несанкціонований доступ до конфіденційної інформації. Умови функціонування СІБ з метою попередження та ліквідації зазначених небезпек представлено на рис. 2.14 – 2.15.

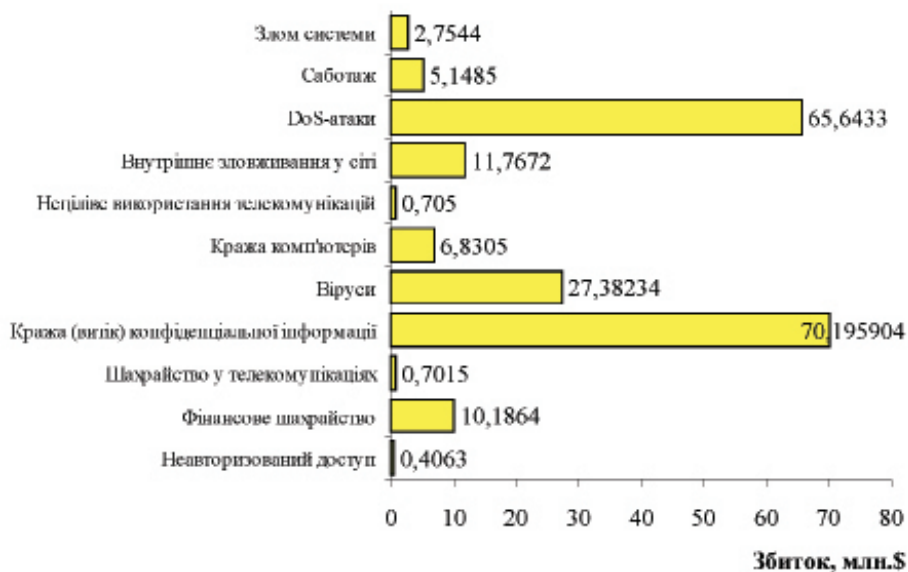


Рис. 2.13 – Розмір збитку підприємств за видами атак на інформацію що оберталась у процесі їх діяльності у 2003 р. за даними CSI/FBI Computer Crime and Security Survey

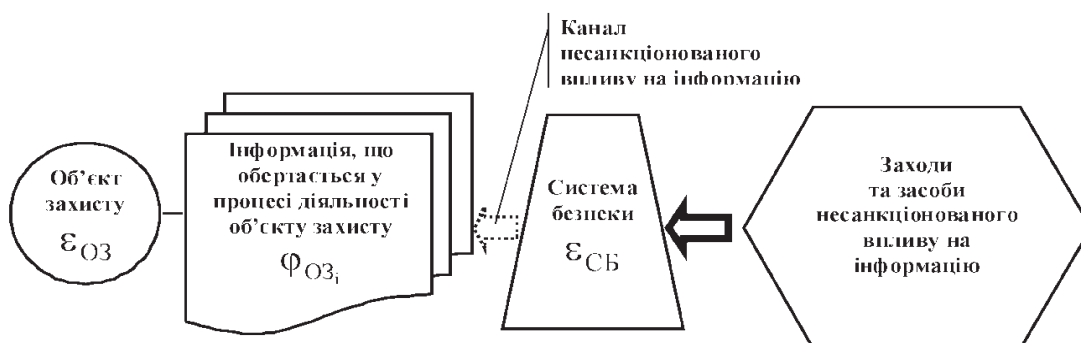


Рис. 2.14 – Схема функціонування елемента „інформаційна безпека” системи інтегральної безпеки з метою недопущення несанкціонованого впливу на інформацію, що обертается у процесі діяльності об'єкту захисту

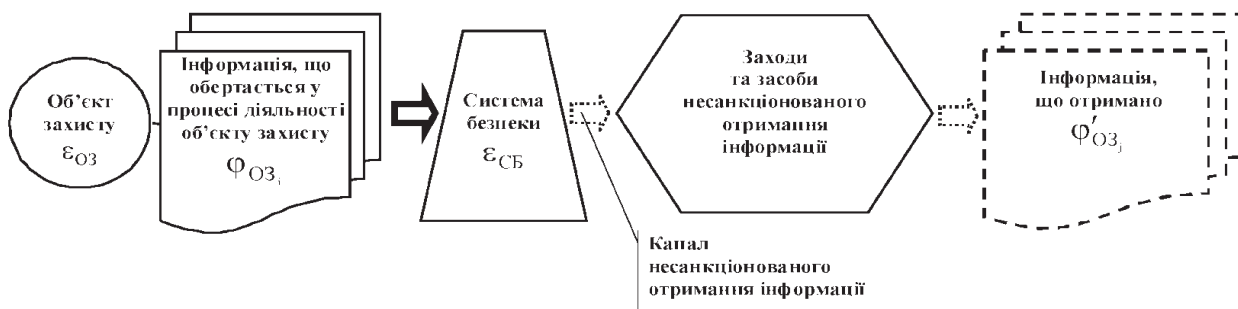


Рис. 2.15 – Схема функціонування елемента „інформаційна безпека” системи інтегральної безпеки з метою недопущення несанкціонованого доступу до інформації, що обертается у процесі діяльності об'єкту захисту

В межах складової «інформаційна безпека» можливо визначити наступні напрямки заходів її реалізації – рис. 2.16.

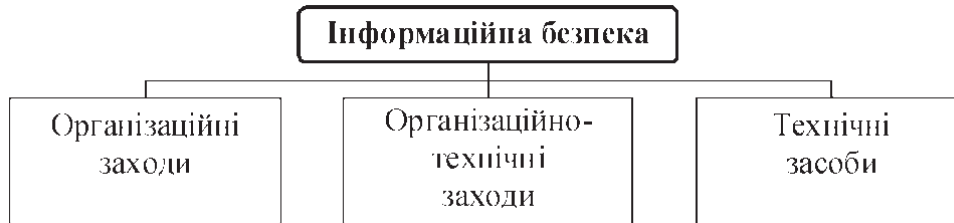


Рис. 2.16 – Структура елемента «інформаційна безпека» системи інтегральної безпеки

Затрати на реалізацію даного елемента СІБ складають:

$$S^{(ІБ)} = S_{орг.}^{(ІБ)} + S_{орг.-тех}^{(ІБ)} + S_{тех}^{(ІБ)}, \quad (2.6)$$

В залежності від характеристик об’єкту, наявності небезпек, їх природи та інших складових визначаються пріоритети щодо розбудови загальної спрямованості складової «інформаційна безпека», що з свого боку визначає вагомість внеску відповідних заходів (2.6) – табл. 2.11.

Таблиця 2.11 – Вагомість заходів складової «інформаційна безпека» системи інтегральної безпеки у розподілі економічного потенціалу

Економічний потенціал	Система безпеки
$S_{орг.}^{(ІБ)} \uparrow + S_{орг.-тех}^{(ІБ)} + S_{тех}^{(ІБ)}$	орієнтована на організаційні заходи
$S_{орг.}^{(ІБ)} + S_{орг.-тех}^{(ІБ)} \uparrow + S_{тех}^{(ІБ)}$	орієнтована на організаційно-технічні заходи
$S_{орг.}^{(ІБ)} + S_{орг.-тех}^{(ІБ)} + S_{тех}^{(ІБ)} \uparrow$	орієнтована на технічні заходи
$S_{орг.}^{(ІБ)} \approx S_{орг.-тех}^{(ІБ)} \approx S_{тех}^{(ІБ)}$	рівно зорієнтована

Так для комплектації підсистеми «інформаційна безпека» технічними засобами захисту від несанкціонованого доступу маємо:

$$S_{\text{техн.}}^{(ІБ)} = S_{T_1}^{(ІБ)} + S_{T_2}^{(ІБ)} + S_{T_3}^{(ІБ)}, \quad (2.7)$$

де $S_{T_1}^{(ІБ)}$ – складова ціни засобу попередження небезпеки, яка обумовлена властивостями каналів несанкціонований доступ до інформації (рис. 2.17); $S_{T_2}^{(ІБ)}$ – складова ціни засобу попередження небезпеки, яка обумовлена вибором типу технічного засобу (рис. 2.18); $S_{T_3}^{(ІБ)}$ – складова ціни засобу попередження небезпеки, яка обумовлена його технічними характеристиками.

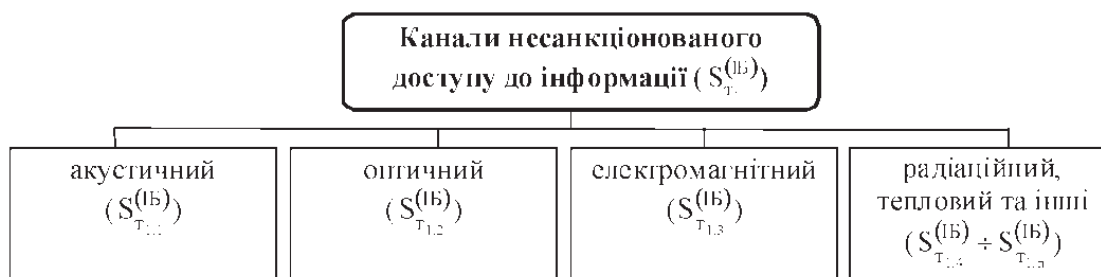


Рис. 2.17 – Загальна структура каналів несанкціонованого доступу до інформації

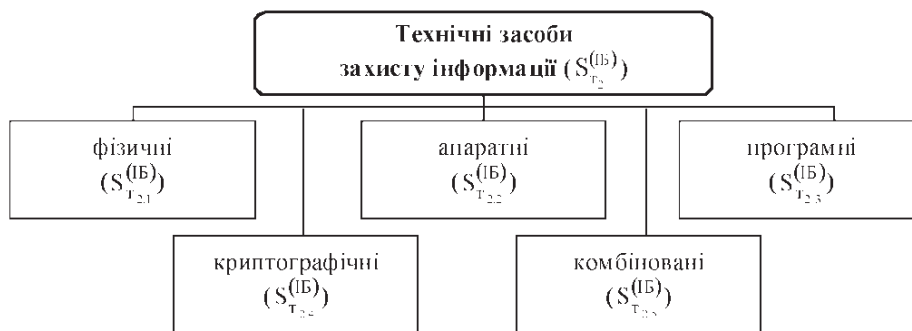


Рис. 2.18 – Загальна структура технічних засобів з захисту інформації від несанкціонованого доступу

Апаратні засоби з захисту інформації від несанкціонованого доступу об'єднують технічні засоби, які за принципом роботи, будовою та можливостями виявляють канали витoku інформації та протидіють їх функціонуванню. Таким чином, апаратні засоби захисту інформації використовуються для вирішення наступних задач:

- проведення досліджень технічних засобів, що використовуються у процесі діяльності ОЗ, на наявність можливих каналів витоку інформації;
- виявлення каналів витоку інформації на різного роду ОЗ та у приміщеннях, які входять до його структури;
- локалізація каналів витоку інформації;
- пошук та виявлення засобів витоку інформації;
- протидія несанкціонованому доступу до джерела інформації, що захищається.

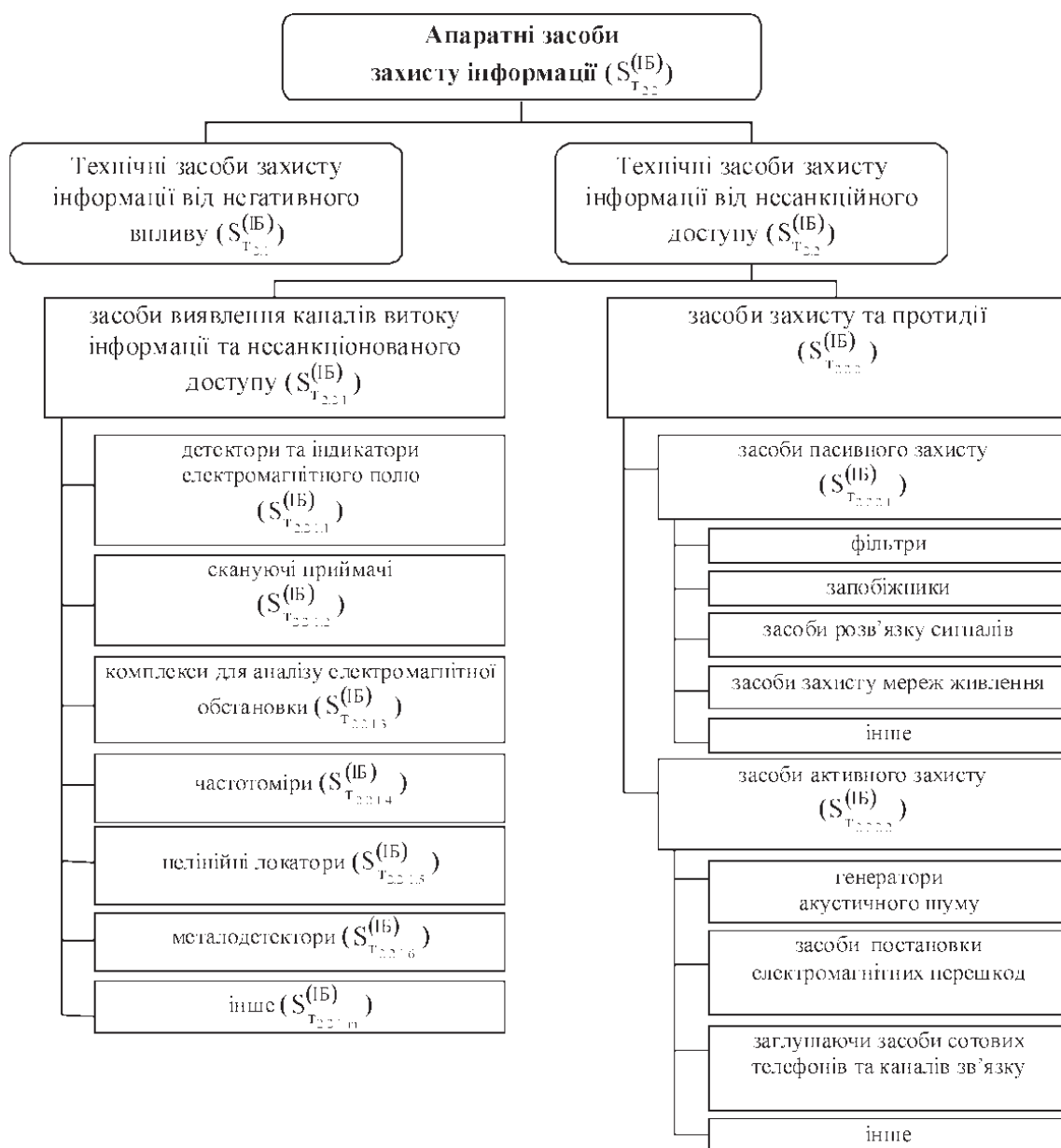


Рис. 2.19 – Загальна структура технічних засобів з захисту інформації

За функціональним призначенням апаратні засоби з захисту інформації від несанкціонованого доступу класифікуються на засоби виявлення, засоби пошуку і детальних вимірювань, засоби активної і пасивної протидії (рис. 2.19). При цьому, за технічними можливостями апаратні засоби з захисту інформації від несанкціонованого доступу виступають як засоби загального призначення для проведення попередніх оцінок, так і професійні комплекси для проведення досконалого пошуку, виявлення та детального вимірювання технічних характеристик засобів витоку інформації. Однак, вплив на складову $S_{T_2}^{(ІБ)}$ даної структуризації апаратних засобів з захисту інформації від несанкціонованого доступу та неможливість побудови універсальної системи безпеки відкриває перед спеціалістами з розробки систем безпеки проблему оптимальної, наряду з іншими складовими (рис. 2.16), комплектації технічними засобами складової «інформаційна безпека» СІБ ОЗ за критерієм «ефективність – інтегральна ціна».

За наведеним критерієм проведено аналіз апаратних засобів виявлення радіо каналу несанкціонованого доступу до інформації [79 – 99, 102, 103]. Результати представлено у табл. 2.12 – 3.14 та узагальнено на рис. 2.20.

Таблиця 2.12 – Засоби виявлення каналів витоку інформації. Характеристики детекторів та індикаторів електромагнітного поля

Найменування приладу	Пріоритетна характеристика (робочий діапазон, МГц)	Ціна	
		кількісна, у.о.	якісна
RD-11	100 ÷ 6000	144	$S_{T_{1,3}}^{(ІБ)} + \bar{S}_{T_{2,2.1.1}}^{(ІБ)} + \bar{S}_{T_3}^{(ІБ)}$
PROTECT 1203	10 ÷ 3600	210	
«Зажигалка»	54 ÷ 7200	278	
PROTECT 1205	30 ÷ 2400	286	
PROTECT 1206	50 ÷ 3600	490	
• • •			

Примітка: $S_{...}$ – базовий показник ціни; $\bar{S}_{...}$ – домінуюча складова ціни

Таблиця 2.13 – Засоби виявлення каналів витоку інформації. Характеристики скакуючих приймачів

Найменування приладу	Пріоритетні характеристики			Ціна	
	робочий діапазон, МГц	чутливість, мкВ	тип модуляції	кількісна, у.о.	якісна
IC-R5	10 ÷ 1310	–	NFM, WFM, AM	316	$S_{T_{1,3}}^{(ІБ)}$ + $+\bar{S}_{T_{2,2.1,2}}^{(ІБ)}$ + $+\bar{S}_{T_3}^{(ІБ)}$
AR-8200 МКЗ	0,1 ÷ 3000	не гірше 0,3	WFM, FM, SFM (Wide, Narrow, Super FM); WAM, AM, NAM (Wide, Standard, Narrow AM); USB, LSB, CW	625	
IC-R20	0,15 ÷ 3300	не гірше 0,32	усі типи модуляції	726	
• • •					
стаціонарні					
AR8600 Mk2	0,1 ÷ 3300	не гірше 0,3	усі типи модуляції + 3 додаткових	1112	
AR3000A	0,1 ÷ 2000	не гірше 0,25	усі типи модуляції	1580	
AR5000A	0,01 ÷ 3000	не гірше 0,14	усі типи модуляції	2292	
AR5000	0,01 ÷ 2600	не гірше 0,14	усі типи модуляції	2458	
• • •					

Таблиця 2.14 – Засоби виявлення каналів витоку інформації. Характеристики комплексів для аналізу електромагнітної обстановки

Найменування приладу	Пріоритетні характеристики			Ціна	
	робочий діапазон, МГц	чутливість, мкВ	швидкість обзору, МГц/с	кількісна, у.о.	якісна
Спектр-МК	40 ÷ 3000	не гірше 2	до 100	18945	$S_{T_{1,3}}^{(ІБ)}$ + $+\bar{S}_{T_{2,2.1,3}}^{(ІБ)}$ + $+\bar{S}_{T_3}^{(ІБ)}$
С2М «Квадрат»	40 ÷ 6000	не гірше 2	до 100	19336	
Омега	2000 ÷ 18000	не гірше 2	до 350	23047	
• • •					

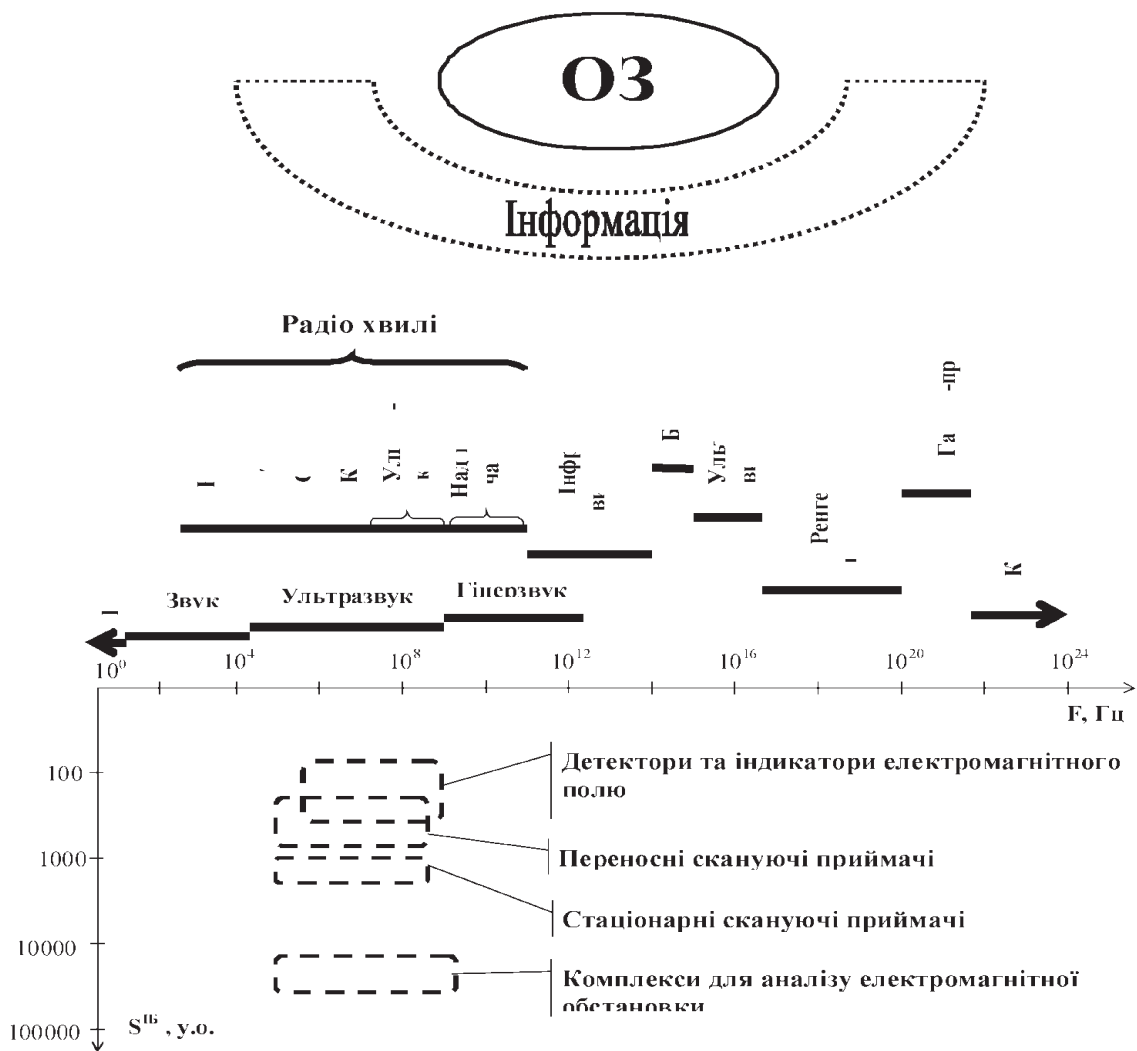


Рис. 2.20 – Графічне представлення областей функціонування технічних засобів виявлення витoku інформації по електромагнітному каналу несанкціонованого доступу в залежності від пропускної частоти каналу (F)

2.6. Алгоритм формування технічної бази системи інтегральної безпеки

Узагальнення процедури застосування наведеного критерію (розділи 2.4 та 2.5) дає змогу визначити наступний алгоритм дій щодо формування технічної бази системи інтегральної безпеки об'єкту захисту:

- 1) провести аналіз можливого спектру небезпек, які мають місце у разі виникнення надзвичайної події даного типу (нерегламентованого режиму функціонування);
- 2) сформуванати графічну (або аналітичну) залежність між фактором небезпе-

- ки та пріоритетними характеристиками наявних технічних засобів (рис. 2.11, 2.12, 2.20) в одиницях «безпека – втрати»;
- 3) виходячи з вимог безпеки об'єкту захисту, визначити пріоритетний фактор небезпеки, що і обумовлює утворення складової «інтегральна ціна» ($S_{п_{т1}}^{(i)}$) – рис. 2.21;
- 4) складові $S_{п_{т2}}^{(i)}$ та $S_{п_{т3}}^{(i)}$ визначаються з вимог технологічного процесу та додаткових вимог, що мають місце на об'єкті захисту (рис. 2.21).

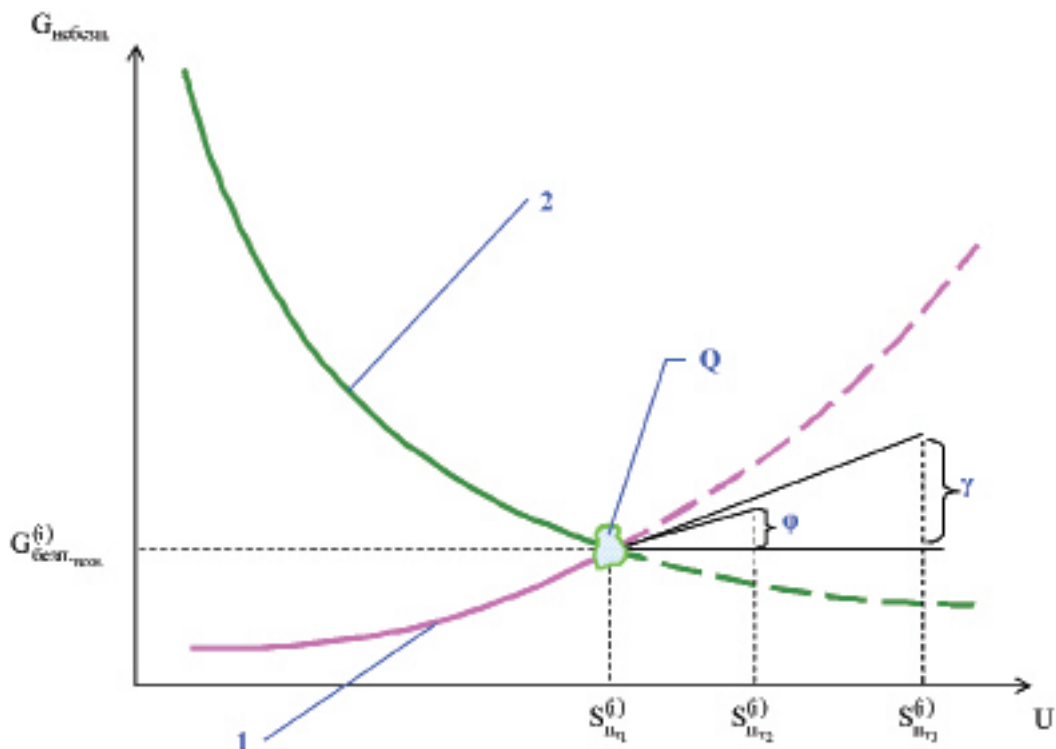


Рис. 2.21 – Залежність рівня безпеки від вибору технічних засобів безпеки та затрат пов'язаних з профілактикою прояви і-ої небезпеки ($G_{небезп.}$ – рівень небезпеки; U – розмір втрат; $G_{безп.техн.}^{(i)}$ – рівень безпеки, який досягається за допомогою вибраного типу технічного засобу; 1 – крива, яка характеризує динаміку пріоритетного фактору і-ої небезпеки; 2 – пріоритетна характеристика технічного засобу (сімейство кривих); Q – область вияву небезпеки; ϕ – приріст рівня безпеки за умов врахування додаткових необхідних технічних вимог (надійність, періодичність роботи та інше); γ – приріст рівня безпеки за умов врахування додаткових необхідних вимог об'єкту контролю (вибухонебезпечне виконання та інше)

Слід зазначити, що при розробці засобів безпеки, на відміну від безпосереднього комплектування СІБ технічними засобами, домінуючою є пріоритетна характеристика, розробка або підвищення її ефективності у взаємовпливі з іншими характеристиками і визначає ефективність заходів (досліджень). У разі формування СІБ технічними засобами безпеки критерієм виступає інтегральна ціна, яка складається із ціни всіх наведених раніше показників (пріоритетних та додаткових), що пов'язано з неможливістю (у багатьох випадках недоцільністю) покращити вже існуючі пріоритетні характеристики сертифікованої та запущеної на ринок продукції без додаткових наукових та економічних затрат. Відсутність даного типу засобів безпеки з необхідними пріоритетними технічними показниками переводить задачу вибору до іншого типу технічних засобів.

ЛІТЕРАТУРА

1. Ожегов С.И. Словарь русского языка / Под ред. Член. корр. АН СССР Н.Ю.Шведовой. – М.: Русский язык, 1985. – 796 с.
2. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2002 році” – К.:Чорнобильінтерінформ, 2003. – 291 с.
3. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2003 році” – К.:Чорнобильінтерінформ, 2004. – 435 с.
4. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2004 році” – К.:Чорнобильінтерінформ, 2005. – 360 с.
5. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2005 році” – К.:Чорнобильінтерінформ, 2006. – 375 с.
6. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2006 році” – К.:Чорнобильінтерінформ, 2007. – 236 с.
7. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2007 році” – К.:Чорнобильінтерінформ, 2008. – 230 с.
8. Національна доповідь „Про стан техногенної та природної безпеки в Україні у 2008 році” (www.mns.gov.ua)
9. Абрамов Ю.О., Грінченко Є.М., Кірючкін О.Ю. та інші Моніторинг надзвичайних ситуацій. –Харків, АЦЗУ, 2005. – 530 с.
10. Акимов В.А., Новиков В.Д., Радаев Н.Н. Природные и техногенные чрезвычайные ситуации: опасности, угрозы, риски. – М.: «Деловой экспресс», 2001. – 304 с.
11. Махутов Н.А., Петров В.П., Ахметханов Р.С. Природно-техногенно-социальные системы и риски // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2004. – Вып. 3. – С. 3 – 30.
12. Дзюндзюк Б.В., Хяникяйнен А.И., Швед В.Б. Катастрофы и чрезвычайные ситуации. – Харьков: Форт, 1998. – 120 с.
13. Акимов В.А., Гудыно П.В., Потапов Б.В., Радаев Н.Н. Расчет риска технологических катастроф, инициированных природными явлениями // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2000. – Вып. 1. – С. 38 – 48.
14. Махутов Н.А., Гаденин М.М. Стратегические риски в техногенной сфере // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2003. – Вып. 4. – С. 10 –

20.

15. Качинский А.Б., Агаркова Н.В. Исследование тенденций и характера изменений чрезвычайных ситуаций в Украине // Проблемы упр. и информатики. – 2002. – № 5. – С. 127 – 136.
16. ЗУ „Про правові засади цивільного захисту” (www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi)
17. Шоботов В.М. Цивільна оборона. – Київ: Центр навчальної літератури, 2004. – 439 с.
18. Кононов Д.А., Кульба В.В., Малинецкий Г.Г. Сценарий поведения сложных систем в чрезвычайных ситуациях // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2001. – Вып. 5. – С. 4 – 19.
19. Моляко В.А. Особенности проявления паники в условиях экологического бедствия (на примере Чернобыльской атомной катастрофы) // Психологический журнал. – 1992. – № 2. – С. 66 – 74.
20. Евграфов П.М., Нестеров А.В., Нестерова О.В. Подготовка населения к действиям при пожарах как единая информационно-техническая и психологическая проблема // Пожаровзрывобезопасность. – 2008. – № 5. – С. 5 – 15.
21. Тютюник В.В., Шевченко Р.І., Тютюник О.В. Оцінка індивідуальної небезпеки населення регіонів України в умовах надзвичайних ситуацій // Проблеми надзвичайних ситуацій. Зб. наук. пр. – Харків: УЦЗУ, 2009. – Вип. 9. – С. 146 – 157.
22. Диллон Б., Сингх Ч. Инженерные методы обеспечения надежности систем – М.: Мир, 1984. – 318 с.
23. Топольский Н.Г., Блудчий Н.П. Потенциальная опасность массового поражения при крупных техногенных авариях – М.: ВИПТШ МВД России, 1994. – 75 с.
24. ЗУ „Про основи національної безпеки України” (www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi)
25. Горбулин В. Безопасность – 2010 // Зеркало недели. – 2006. – № 48(627). – 16 – 22 декабря. (www.zn.ua/1000/1030/55351/)
26. Воронков Л.С. Региональные аспекты безопасности Украины (www.niurr.gov.ua/ru/conference/sevastopol_conf/voronkov.htm)
27. Рыжова Л.А. Обзор перспективных направлений развития науки и техники

-
-
- в области безопасности // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 6. – С. 124 – 127.
28. Бро Г.В., Пожитной Н.М. К теории безопасности земной цивилизации (фил.-социолог. аспект) // Безоп. информ. техн. – 1998. – № 1. – С. 97.
29. Кондратьев В.Д., Толстых А.В., Уандыков Б.К., Щепкин А.В. Комплексная оценка уровня риска опасного объекта // Системы управления и информац. технологий. – 2004. – № 3(15). – С. 53 – 57.
30. Капранов М. Комплексный подход к проблемам тушения объектов с автоматической противопожарной защитой // Алгоритм. безопас. – 2007. – № 5. – С. 28 – 31.
31. Кірочкін О.Ю., Левтеров О.А., Тютюник В.В., Шевченко Р.І. Формування інтегральної системи безпеки – запорука добробуту України // F+S: технології безпеки і протипожежної захити. – 2008. – № 6(36). – С. 60 – 63.
32. Гражданкин А.И., Белов П.Г. Экспертная система оценки техногенного риска опасных производственных объектов // Безопасность труда в промышленности. – 2000. -№ 11. – С. 6-10
33. Марченко П.Е. Построение интегральных оценок природно-техногенной опасности территорий // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 4. – С. 91 – 98.
34. Махутов Н.А., Резников Д.О., Петров В.П. Оценка риска аварий на КВО с учетом возможности реализаций экстремальных ущербов // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 5. – С. 57 – 73.
35. Абрамов Ю.А., Росоха В.Е., Тютюник В.В., Чучковский В.Н., Шевченко Р.И. Основы мониторинга и управления в условиях чрезвычайных ситуаций. – Х.: Изд. АГЗУ, 2005. – 257 с.
36. Мовою науки. Результати дослідження пожежних ризиків в Україні // Будівництво та безпека. – 2008. – № 3(7). – С. 6 – 7.
37. Грінченко Є.М., Кірочкін О.Ю., Тютюник В.В., Шевченко Р.І. Інтегральна система безпеки регіонів України, як складових державної територіально-часової параметричної системи. Принцип комплексної оцінки небезпеки // Проблеми надзвичайних ситуацій. – Харків: УЦЗУ, 2008. – Вип. 7. – С. 58 – 71.

-
-
38. Порфирьев Б.Н. Совершенствование управления региональной безопасностью в природно-техногенной сфере // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2004. – № 3. – С. 3 – 30.
 39. Лепихин А.М. Комплексные показатели безопасности территорий // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 5. – С. 93 – 98.
 40. Агишев Р.Р., Власов В.А. Оценка эффективности средств дистанционного мониторинга техногенных загрязнений воздуха для обеспечения безопасности промышленных объектов // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2002. – № 6. – С. 22 – 47.
 41. Короленко Ц.П. Психология человека в экстремальных условиях. – М.: Медицина, 1978. – 178 с.
 42. Александровский Ю.А., Лобастов О.С., Спивак Л.И., Щукин Б.П. Психогении в экстремальных условиях. – М.: Медицина, 1991. – 96 с.
 43. Євсюков О.П., Тімченко О.В. Психологічне прогнозування надійності діяльності працівників аварійно-рятувальних підрозділів МНС України. – Харків, 2007. – 288 с.
 44. Гаврилов С.Д., Гавришев М.Ю., Гринев М.П. и др. Количественная оценка рисков вреда здоровью с учетом социальных, экономических и гигиенических факторов // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 2. – С. 3 – 10.
 45. Шидловский Н.П. Совершенствования системы медицинской помощи при чрезвычайных ситуациях // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 2. – С. 82 – 87.
 46. Поликарпов В.С. Философия безопасности. – СПб. – Ростов-на-Дону – Таганрог: Изд-во ТРТУ, 2001 (www.abovo.net.ru/book/98049)
 47. Философия техники (www.zipsites.ru/books/filosofiya_tekhniki)
 48. Бро Г.В., Пожитной Н.М. О концепции общенаучной теории безопасности земной цивилизации на рубеже второго и третьего тысячелетий // Безопасность информационных технологий. – 1998. – № 3. – С. 82 – 83.
 49. Бурков В.Н., Грищенко А.Ф., Кулик О.С. Задачи оптимального управления промышленной безопасностью. – М.: ИПУ РАН, 2000. – 70 с.
 50. Тютюник В.В., Шевченко Р.І. Основні принципи інтегральної системи безпеки при надзвичайних ситуаціях // Зб. наук. праць Харків. ун-ту Повітряних

-
- Сил. – Х.: ХУПС ім. І. Кожедуба, 2008. – Вип. 3(18). – С. 179 – 182.
51. Абрамов Ю.А., Тютюник В.В., Шевченко Р.И. Взаимосвязь иницирующих и поражающих факторов чрезвычайных ситуаций природного характера на территории Украины // Проблемы надзвичайних ситуацій. – Харків: УЦЗУ, 2007. – Вип. 5. – С. 8 – 17.
 52. Абрамов Ю.А., Тютюник В.В., Шевченко Р.И. Основные требования к созданию единой системы мониторингу чрезвычайных ситуаций // Системи обробки інформації. – Харків: ХУПС. – 2005. – Вип. 6(46). – С. 203 – 207.
 53. Хенли Э.Дж., Кумамото Х. Надежность технических систем и оценка риска: Пер. с англ. В.С. Сыромятникова, Г.С. Деминой. Под общ. ред. В.С. Сыромятникова. – М.: Машиностроение, 1984. – 528 с.
 54. Репин В.И. Интеллектуальное здание. Проблемы и решения // Стройпрофиль. – 2001. – № 9. (www.ista.ru)
 55. Шевченко Р.І., Одарюк П.В., Тютюник В.В. Оцінка ефективності інтегрованої системи безпеки функціонування підприємств нафтопереробної промисловості // Проблемы пожарной безопасности. – Харьков: Фолио, 2005. – Вып. 18. – С. 185 – 191.
 56. Омельчук А.М. Интеграция систем безопасности и нелинейность матрицы угроз // Системы безопасности – 2001. – № 41 (октябрь-ноябрь). – С. 20 – 21
 57. Бояринцев А.В., Шумилов Н.И. Анализ уязвимости объектов. Место и роль в создании, модернизации и оценке эффективности систем обеспечения безопасности // Системы безопасности – № 42 (декабрь 2001 – январь 2002). – С. 42 – 43.
 58. Мусиенко Д. Экспертиза безопасности объекта // Бизнес и безопасность. – 2006. – № 6. – С. 3 – 5.
 59. Кондратьев В.Д., Толстых А.В., Уандыков Б.К., Щепкин А.В. Комплексная оценка уровня риска опасного объекта // Системы управления и информац. технологии. – 2004. – № 3 (15). – С. 53 – 57.
 60. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2003. – 352 с.
 61. Бешелев С.Д., Гурвич Ф.Г. Математико-статистичні методи експертних оцінок. – М.: Статистика, 1974. – 264 с.
 62. Бурков В.Н., Панкова Л.А., Шнейдерман М.В. Получение и анализ экспертной

інформації. – М.: ІПУ, 1980. – 50 с.

63. Тютюник В.В., Шевченко Р.І. Формування критерію „ефективність” – „інтегральна ціна”, як основи принципу комплектування технічними засобами інтегральної системи безпеки // Проблемы пожарной безопасности. – Харьков: УГЗУ, 2008. – Вып. 23. – С. 202 – 216.
64. Шепитько Г.Е., Гудов Г.Н., Медведев И.И. Прогноз рентабельности системы комплексной безопасности предприятия // Системы безопасности – 2003. Материалы XII науч.-техн. конф. – Москва, 2003. – С. 82 – 85.
65. Карпычев В.Ю., Кузнецов В.А. Основные экономические подходы к созданию систем безопасности // Системы безопасности – 2004. Материалы XIII науч.-техн. конф. – Москва, 2004. – С. 126 – 128.
66. Україна в 2008 році: процеси, результати, перспективи. Біла книга державної політики / За заг. ред. Ю.Г. Рубана. – К.: НІСД, 2008. – 186 с.
67. Маршалл В. Основне опасности химических производств /Пер. с англ. –М.: Мир, 1989. – 672 с.
68. Небезпечні хімічні речовини в природі, промисловості і побуті. Довідник – К.: Чорнобильінтерінформ, 1998, - 452 с.
69. Методичні рекомендації з класифікації надзвичайних ситуацій – К.: МНС України, 2004. – 65 с.
70. Дубров А.М., Мхитарян В.С., Трошин Л.И. Многомерные статистические методы – М.: «Финансы и статистика», 1998, - 340 с.
71. Абрамов Ю.О., Тютюник В.В., Шевченко Р.І. Аналіз хімічно небезпечного стану регіонів України // Проблеми надзвичайних ситуацій. – Харків: УЦЗУ, 2006. – Вип. 4. – С. 16 – 29.
72. Кірючкін О.Ю., Мурін М.М., Тютюник В.В., Шевченко Р.І. Оцінка багатокритеріальної методики аналізу хімічно небезпечного стану об’єктів та регіонів України // Проблеми надзвичайних ситуацій. – Харків: УЦЗУ, 2007. – Вип. 6. – С. 62 – 73.
73. Кірючкін О.Ю., Левтеров О.А., Тютюник В.В., Шевченко Р.І. Застосування концепції інтегральної системи безпеки до аналізу хімічно небезпечного стану регіонів України // F+S: технологии безопасности и противопожарной защиты. – 2009. – № 1(37). – С. 80 – 84.
74. Черняховский Э.Р., Шкидченко А.Н., Юматова О.А., Чушкина З.Ю.

-
-
- Применение различных технологий при ликвидации последствий аварийных разливов нефти, нефтепродуктов и продуктов нефтесодержащих отходов // ВИНТИ. Пробл. безоп. при чрезв. ситуациях. – 2005. – вып. 2. – С. 34 – 41.
75. Миронюк С.Г. Концепция мониторинга чрезвычайных ситуаций техногенного характера на объектах обустройства нефтяных месторождений // Пробл. безопасн. и чрезв. ситуации. – 2008. – № 5. – С. 18 – 26.
76. Соколов В.С. Системы пожарной сигнализации и автоматики. Боевая эффективность. Соотношения цена/качество // Системы безопасности – 2001. – № 41 (октябрь-ноябрь). – С. 54 – 58.
77. Моисеев И.Ф. Рынок противопожарного оборудования. Взгляд изнутри // Системы безопасности – 2001. – № 41 (октябрь-ноябрь). – С. 71.
78. Членов А.Н., Землянухин М.В., Родионов А.В. Анализ тенденций развития технических средств пожарной сигнализации // Системы безопасности – 2004. Материалы XIII науч.-техн. конф. – Москва, 2004. – С. 220 – 223.
79. Офіційний каталог IV Міжнародного виставкового форуму «Технології захисту – 2005». – Київ, 2005. – 166 с.
80. Офіційний каталог Міжнародної спеціалізованої виставки «ПОЖТЕХ – 2007». – Київ, 2007. – 128 с.
81. Офіційний каталог VI Міжнародного виставкового форуму «Технології захисту – 2007». – Київ, 2007. – 142 с.
82. Офіційний каталог Міжнародної спеціалізованої виставки «ПОЖТЕХ – 2008». – Київ, 2008. – 170 с.
83. Офіційний каталог VII Міжнародного виставкового форуму «Технології захисту – 2008». – Київ, 2008. – 132 с.
84. Офіційний каталог Міжнародної спеціалізованої виставки «ПОЖТЕХ – 2009». – Київ, 2009. – 126 с.
85. www.magazine.security.com.ua
86. www.security-info.com.ua
87. www.securpress.ru
88. www.kiev-security.org.ua
89. www.opta.com.ua
90. www.arsenal-sb.ru

-
-
91. www.das.kiev.ua
 92. www.klad.com.ua
 93. www.bezpeka.com
 94. www.magazine.security.com.ua
 95. www.security-info.com.ua
 96. www.shop.sec.ru
 97. www.techportal.ru
 98. www.price.security-bridge.com
 99. www.centres.ru
 100. Каталог пожарная безопасность. Оборудование, проектирование, монтаж. – Киев, 2000. – 128 с.
 101. www.secretssaver.com/news/news1.html
 102. Черешкин Д.С., Гадасин В.А., Елизаров О.И. и др. Оценка эффективности систем защиты информационных ресурсов. – М.: Ин-тут системного анализа РАН, 1998.
 103. Тютюник В.В., Шевченко Р.І. Принцип комплектування технічними засобами складової „інформаційна безпека” інтегральної системи безпеки за критерієм „ефективність – інтегральна ціна” // Системи озброєння і військова техніка. Наук. журнал. – Харків: ХУПС ім. І. Кожедуба, 2009. – № 2(18). – С. 159 – 165.

ЗМІСТ

ВСТУП.....	3
1. СИСТЕМА ІНТЕГРАЛЬНОЇ БЕЗПЕКИ ІЗ ЗАПОБІГАННЯ ЕКСТРЕМАЛЬНИХ ТА НАДЗВИЧАЙНИХ СИТУАЦІЙ.....	9
1.1. Концепція системи інтегральної безпеки. Основні принципи побудови елементів системи.....	9
1.2. Функції та структура системи інтегральної безпеки.....	12
1.3. Принцип комплексної оцінки інтегральної безпеки об'єктів захисту регіонального рівня	20
1.4. Принцип комплексної оцінки стану інтегральної безпеки об'єктового рівня	25
1.5. Принцип комплектування технічними засобами системи інтегральної безпеки.....	29
2. ЗАСТОСУВАННЯ КОНЦЕПЦІЇ ІНТЕГРАЛЬНОЇ БЕЗПЕКИ	33
2.1. Застосування концепції інтегральної безпеки для оцінки стану регіонів України (на прикладі «небезпека від надзвичайних ситуацій техногенного та природного характеру»).....	33
2.2. Застосування концепції інтегральної безпеки для оцінки стану регіонів України (на прикладі «хімічна небезпека»)	39
2.3. Застосування концепції інтегральної безпеки для оцінки безпеки функціонування підприємства (на прикладі підприємств нафтопереробної промисловості).....	49
2.4. Застосування концепції інтегральної безпеки для комплектування технічними засобами (на прикладі «пожежна безпека»).....	51
2.5. Застосування концепції інтегральної безпеки для комплектування технічними засобами (на прикладі «інформаційна безпека»).....	59
2.6. Алгоритм формування технічної бази системи інтегральної безпеки.....	66
ЛІТЕРАТУРА	69

Наукове видання

Тютюник Вадим Володимирович

Шевченко Роман Іванович

СИСТЕМА ІНТЕГРАЛЬНОЇ БЕЗПЕКИ ОБ'ЄКТІВ ЗАХИСТУ

Монографія

Підписано до друку 23.12.2009. Формат 60×84^{1/16}.
Папір офсетний. Друк ризогр. Ум. друк. арк. 4,50.
Обл.-вид. арк. 4,45. Тираж 300 прим. Зам. 643

Видавництво Університету цивільного захисту України.
Україна, 61023, м. Харків, вул. Чернишевського, 94.
Свідоцтво серії __ № __ від „__” _____ р.