УДК 004.05

Домарєв В.В.

СИСТЕМА МОНІТОРИНГУ СТАНУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ НА ОСНОВІ МОДЕЛІ КОМПЛЕКСНОЇ ОЦІНКИ З ВИКОРИСТАННЯМ ІНТЕГРОВАНИХ ПОКАЗНИКІВ.

Сучасна епоха побудови суспільства, в якому за рахунок розвитку продуктивних сил більшість працездатного населення залучена до інформаційної сфери, сприяє розвитку нових форм і методів досягнення країнами політичних, економічних та інших цілей на інформаційному рівні.

Зрозуміло, що зміни, які несе з собою нова епоха позначаються на всіх аспектах як суспільного так і особистого життя людей. Дуже важливо проводити моніторинг таких змін, тобто своєчасно їх спостерігати, оцінювати, прогнозувати та включати в управлінські рішення.

Стан національної безпеки в інформаційній сфері, іншими словами інформаційної безпеки (далі ІБ), визначається системою взаємопов'язаних показників. Існуючі підходи і методики оцінки використовують лише часткові показники окремих питань національної безпеки в інформаційній сфері. Таке становище не дозволяє виявляти закономірності взаємопов'язаних процесів та явищ, прогнозувати їх розвиток з метою формування ефективних рішень щодо протидії загрозам в інформаційній сфері.

Зважаючи на це пропонується варіант системи моніторингу стану національної безпеки в інформаційній сфері на основі моделі комплексної оцінки з використанням системних (інтегрованих) показників.

Зрозуміло, що система моніторингу поряд з іншими складовими повинна мати такі види забезпечення як: інформаційно-аналітичне, програмно-технічне телекомунікаційне, а також наукове супроводження.

Основою системи моніторингу вважається модель оцінки та прогнозування рівня інформаційної безпеки.

Структура запропонованого варіанту системи моніторингу показана на малюнку 1.

Складовими моделі оцінки є:

- математичний апарат (на основі нечітких множин або Fuzzy-технологій),
- комплект методик представлення та розрахунків експертних даних,
- програмний комплекс контент-моніторингу для автоматизації процесів оцінки.

Структура моделі оцінки стану національної безпеки в інформаційній сфері показана на малюнку 2.

Модель оцінки стану інформаційної безпеки повинна відповідати наступним вимогам:

- забезпечувати системній підхід формування оцінок;
- враховувати взаємний вплив показників (об'єктів, процесів, явищ);
- працювати в умовах невизначеності та недостатності початкової інформації;
- забезпечувати наочність (графічне представлення результатів);
- проста у використанні;
- бути універсальною (оцінює різноманітні процеси та явища);
- забезпечувати можливість адоптації до змін умов функціонування;

Визначення показників оцінки стану інформаційної безпеки з урахуванням коефіцієнтів вагомості є складною науковою задачею. Така задача повинна вирішуватися поступово з набуттям досвіду проведення моніторингу. До того ж зміст показників потребує деталізації, що з одного боку ускладнює процес формування оцінок, але з іншого боку підвищує точність та якість оцінки. Якість оцінки стану національної безпеки визначається повнотою експертних даних.

Для комплексної оцінки рівня захищеності пропонуються використовувати узагальнений показник, що представлений у вигляді матриці оцінок, яка формується за допомогою моделі оцінки стану національної безпеки.

Структура формування матриці оцінок стану національної безпеки в інформаційній сфері показана на малюнку 3.

Експертні знання в матриці оцінок пропонується подати у вигляді груп показників, а саме "основи", "напрямки" та "етапи".

Блок показників ***Основи*** інформаційної безпеки.

001 Законодавча, нормативно-методична, наукова база;

002 Структура органів (кадри), які забезпечують національну безпеку в інформаційній сфері;

003 Комплекс організаційних заходів щодо забезпечення інформаційної безпеки (політика національної безпеки);

004 Методи, способи, засоби, послуги за допомогою яких здійснюється забезпечення національної безпеки в інформаційній сфері .

0х0 Блок показників ***Напрямки (сфери)*** інформаційної безпеки:

010 Інформаційна безпека систем державного управління;

020 Безпека інформаційного суспільства (захист та контроль національного інформаційного простору);

030 Інформаційна боротьба;

040 Безпека інформаційно-телекомунікаційних систем;

050 Безпека засобів масової інформації

060 Інформаційний тероризм.

Треба зазначити, що визначення напрямків й особливостей забезпечення інформаційної безпеки в різних сферах життєдіяльності держави, а також уточнення змісту національних інтересів в інформаційній сфері, є вкрай важливою науковою задачею.

х00 Блок показників ***Етапи*** моніторингу стану інформаційної безпеки:

100 Визначення об'єктів моніторингу (у якості об'єктів виступають суспільство та держава)

200 Визначення загроз…

300 Оцінка загроз та ризиків…

400 Визначення заходів та засобів протидії загрозам…

500 Втілення (реалізація) заходів та засобів подолання загроз…

600 Контроль дієздатності вжитих заходів та засобів (оцінка ефективності)

Вигляд зазначеної матриці оцінок з питань інформаційної безпеки представлено на малюнку 4.

Запропонований підхід до визначення груп показників дозволяє проводити багатоцільовий моніторинг стану інформаційної безпеки (по різних аспектах проблематики). При цьому розглянуті методичні питання оцінки рівня ІБ за сукупністю кількісних і якісних показників та обґрунтовано узагальнений показник $\overline{W}$, що враховує характеристики загроз і часткові показники:

$$\overline{W} = \sum_{i=1}^{n}\sum_{j=1}^{k}\overline{\lambda}_i \Delta q_i \alpha_{ij} \overline{x}_{ij} + \sum_{i=1}^{n}\sum_{j=k+1}^{m}\overline{\lambda}_i \Delta q_i \alpha_{ij} \mu(x_{ij}), \qquad (1)$$

де A - відносна частота появи і- ї загрози, i=1,n ;

$\overline{x}_{ij}$ - відносний збиток (ступінь небезпеки) і- ї загрози,

$$0 \le \Delta q_i \le 1; \quad \sum_{i=1}^{n} \Delta q_i = 1; \tag{2}$$

α_{ij} - важливість j-го показника для усунення і- ї загрози; $j = 1, m$;

$\bar{x}_{ij}$ - нормоване значення j-го кількісного показника для усунення і-ї загрози; $\bar{x}_{ij} \le 1; \quad j = 1, k$;

$\mu(x_{ij})$ - функція належності j-го якісного показника необхідному рівню для усунення j- ї загрози; $0 \le \mu(x_{ij}) \le 1; \quad j = k+1, m$.

Необхідні вихідні дані запропоновано одержувати на основі збору і відпрацьовування експертної інформації з використанням теорії нечітких множин.

Для вибору методів визначення ступеня небезпеки загроз і важливості часткових показників рівня ІБ необхідно враховувати фізичну сутність показників і відносини між ними, складність проведення експертизи і трудомісткість одержання експертної інформації, ступінь погодженості думок експертів, трудомісткість обробки експертних даних.

З урахуванням зазначених факторів пропонується метод Сааті, що базується на формуванні матриці парних порівнянь важливості показників. Відповідно до цього методу необхідно вирішити матричне рівняння

$$(A - \lambda E) \cdot W = 0 \tag{3}$$

де A - матриця парних порівнянь;

E - одинична матриця;

W - власний вектор;

λ - власне значення матриці.

Координати власного вектора W і визначають важливість показників.

Найбільш простим у реалізації є метод, що базується на ідеї розподілу ступеня належності елементів множин з визначеною ознакою відповідно до їхніх рангів, отриманих експертним методом.

Під рангом елемента $x_i \in X$ розуміється число $r_s(x_i)$, що характеризує значимість цього елемента у формуванні властивості, що описується нечітким термом S. Допускаємо, що виконується правило: чим більший ранг елемента, тим більше ступінь належності.

Тоді розподіл ступенів належності задається у вигляді співвідношення:

$$\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} = \ldots = \frac{\mu_n}{r_n}, \tag{4}$$

до якого додається умова нормування

$$\mu_1 + \mu_2 + \ldots + \mu_n = 1, \tag{5}$$

де $r_i = r_s(x_i); \quad \mu_i = \mu_s(x_i); i = 1, n.$

Зі співвідношень (4) і (5) одержуємо систему рівнянь, що дозволяє знаходити значення ступенів належності:

$$\left.\begin{array}{l} (1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \ldots + \frac{r_n}{r_1})^{-1} \\ \mu_1 = (\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \ldots + \frac{r_n}{r_2})^{-1} \\ (\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \ldots + 1)^{-1} \end{array}\right\} \tag{6}$$

На основі аналізу нормативних документів і практичного досвіду розроблена методика систематизації і подання експертних даних у вигляді матриці знань, елементами якої є три групи показників: основи, напрямки та етапи. Приклад матриці знань наведено на рис. 4.

Зокрема, лінгвістична оцінка визначається за формулою

$$B_i = \sum_{j=1}^{m} \alpha_j \sum_{b_j=1}^{n} b_j \mu(n_i, b_j), \qquad (7)$$

де B_i - лінгвістична оцінка якості i-го варіанта КСЗІ;

α_j - "вага" j-го показника якості;

n - число градацій j-го показника ($b_j = 1, n$);

$\mu(n_i, b_j)$ - функція належності n_i-го варіанта КСЗІ b_j-ї градації якості.

Висновки.

Таким чином, за допомогою запропонованого підходу можливе створення системи моніторингу із залученням на загальному методичному рівні широкого кола організацій та фахівців.

Запропонована модель здатна використовуватися в якості:

- механізму формування єдиних вимог до системи моніторингу;
- сукупності взаємопов'язаних показників оцінки рівня інформаційної безпеки, яка дозволяє проводити гнучкий та вибірковий моніторинг;
- гнучкого інструмента моніторингу (оцінки стану інформаційної безпеки та своєчасного прийняття рішень щодо запобігання загрозам національній безпеці);
- моделі подальших наукових досліджень процесів інформаційної безпеки з метою покращення якості та ефективності системи моніторингу.

Використовуючи запропоновану модель моніторингу стану національної безпеки в інформаційній сфері можна починати роботу прямо зараз, але точність оцінки стану безпеки буде низька. Проте, по мірі того як буде формуватися система моніторингу, а вхідна інформація буде наближатися до реального стану безпеки (буде достовірною), точність оцінки буде підвищуватися.

Список літератури:

1. Закон України "Про основи національної безпеки України";
2. Концепція (основи державної політики) національної безпеки України. Постанова ВР України від 16 січня 1997 року, №3/97-ВР.
3. *Герасимов Б.М., Грабовский Г.Г., Рюмшин Н.А.* Нечеткие множества в задачах проектирования, управления и обработки информации. К: Техніка, 2002-140 с.
4. *Герасимов Б.М., Домарєв В.В.* Лінгвістичний підхід до обґрунтування вимог до засобів захисту інформації в інформаційній управляючій системі//Збірник наукових праць Київського інституту управління і зв'язку.-Вип.1.-К.: КІУЗ, 2001.
5. *Домарєв В.В.* Модель комплексної оцінки рівня захищеності автоматизованих систем керування ЗС України//Збірник наукових праць/ ЦНДІ озброєння і військової техніки ЗС України. -Вип.6.-К.:ЦНДІ ОВТ, 2001. Інв. 7569. - С.74-81.
6. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД Диа Софт, 2002. –688с.

Надійшла 2.09.2004р.

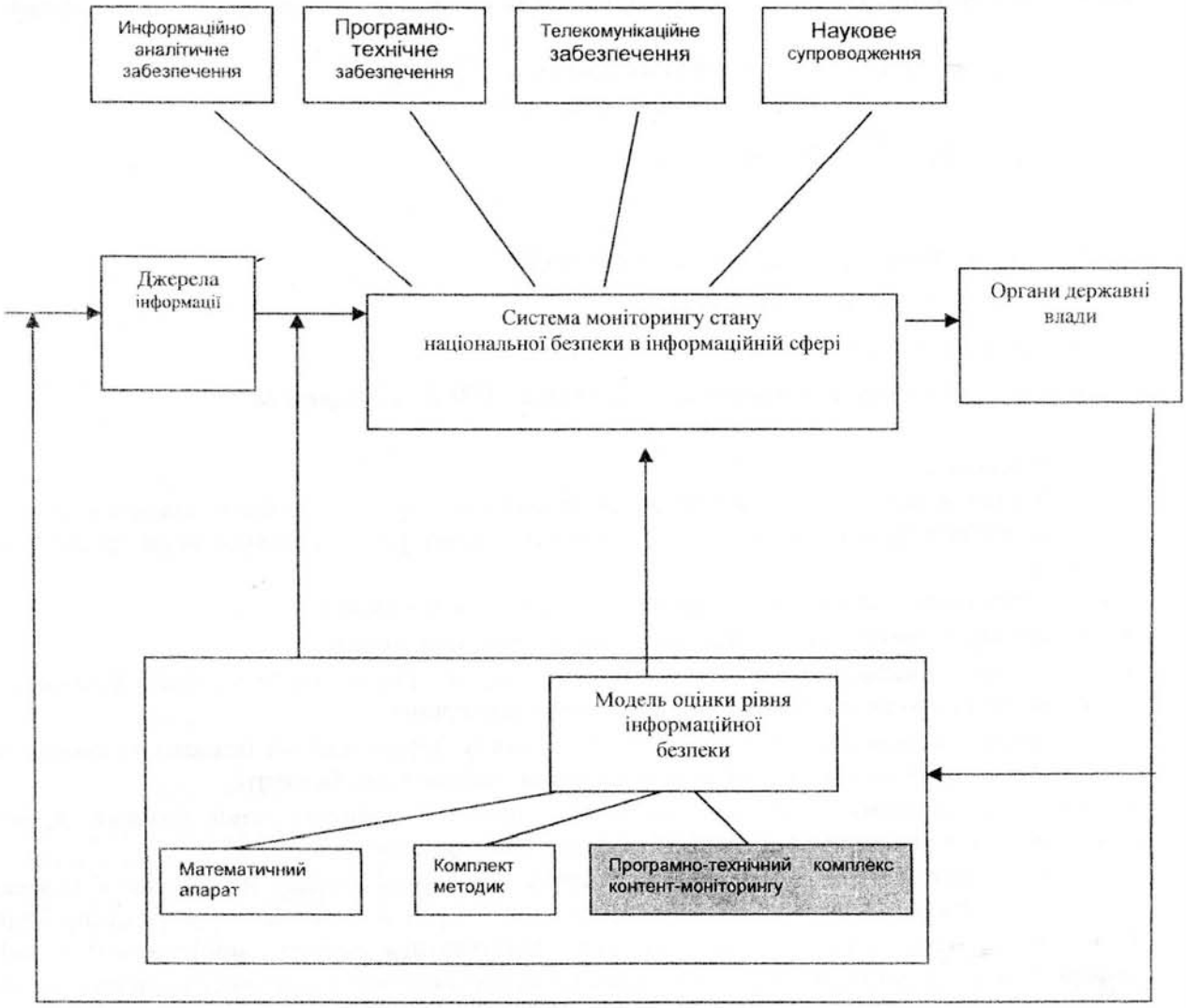

Рис.1. Структура системи моніторингу стану національної безпеки в інформаційній сфері

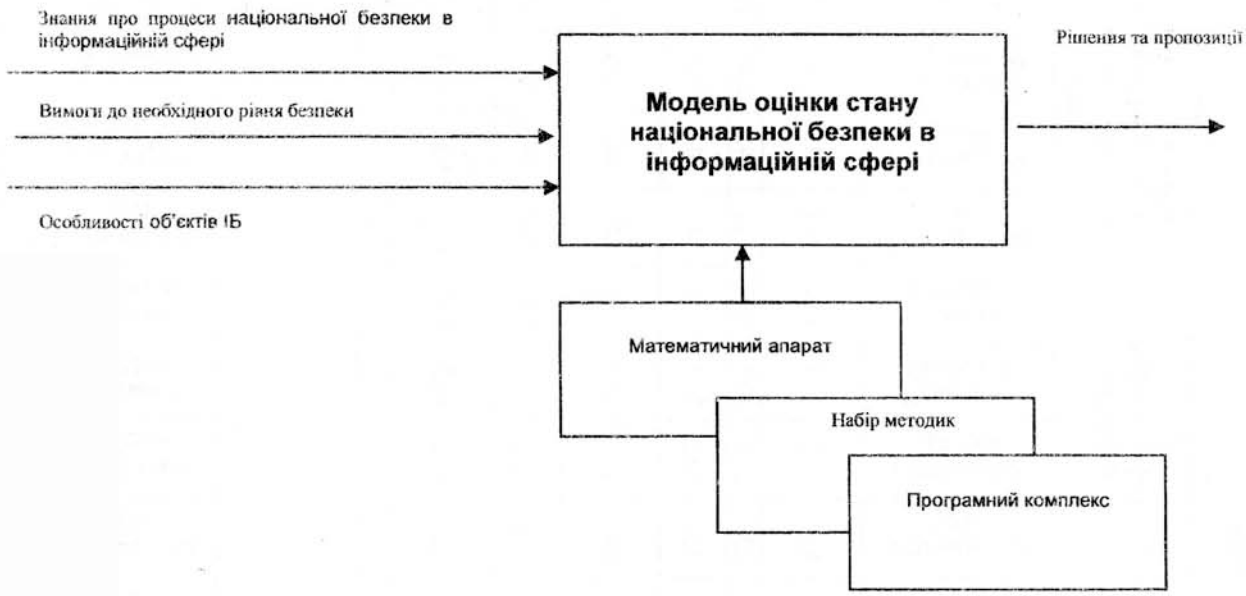

Рис.2. Структура модель оцінки стану національної безпеки в інформаційній сфері

Рис.3. Структура формування матриці оцінок стану безпеки в інформаційній сфері

Матриця оцінок з питань інформаційної безпеки

	Напрямки >>>	010 ІБ державного управління				020 Безпека інформаційного суспільства				030 Інформаційна боротьба				040 Безпека інформаційно-телекомунікаційних систем			
<<<Етапи	Основи >>>	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки
100	Інформаційні ресурси та об'єкти, що потребують захисту (що потребує захисту…)	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144
200	Загрози ІБ (від чого треба захищати…)	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244
300	Вимоги щодо системи ІБ (як повинно бути…)	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344
400	Теоретичні шляхи вирішення проблем ІБ (як можна досягти необхідного рівня безпеки…)	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444
500	Практичні заходи та реалізація (що конкретно треба зробити…)	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544
600	Контроль та оцінка ефективності системи ІБ (керування процесом реалізації запланованих заходів…)	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644

	Напрямки >>>	050 Безпека засобів масової інформації				060 Інформаційний тероризм				070				080			
<<<Етапи	Основи >>>	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки	Нормативна база	Структура органів	Політика безпеки	Заходи безпеки

100	Інформаційні ресурси та об'єкти, що потребують захисту (що потребує захисту…)	151	152	153	154	161	162	163	164	171	172	173	174	181	182	183	184
200	Загрози ІБ (від чого треба захищати…)	251	252	253	254	261	262	263	264	271	272	273	274	281	282	283	284
300	Вимоги щодо системи ІБ (як повинно бути…)	351	352	353	354	361	362	363	364	371	372	373	374	381	382	383	384
400	Теоретичні шляхи вирішення проблем ІБ (як можна досягти необхідного рівня безпеки…)	451	452	453	454	461	462	463	464	471	472	473	474	481	482	483	484
500	Практичні заходи та реалізація (що конкретно треба зробити…)	551	552	553	554	561	562	563	564	571	572	573	574	581	582	583	584
600	Контроль та оцінка ефективності системи ІБ (керування процесом реалізації запланованих заходів…)	651	652	653	654	661	662	663	664	671	672	673	674	681	682	683	684

Рис. 4. Матриця оцінок з питань інформаційної безпеки