УДК 351.861

В.В. Тютюник, Р.І. Шевченко

Університет цивільного захисту України

ПРИНЦИП КОМПЛЕКТУВАННЯ ТЕХНІЧНИМИ ЗАСОБАМИ СКЛАДОВОЇ «ІНФОРМАЦІЙНА БЕЗПЕКА» ІНТЕГРАЛЬНОЇ СИСТЕМИ БЕЗПЕКИ ЗА КРИТЕРІЄМ «ЕФЕКТИВНІСТЬ – ІНТЕГРАЛЬНА ЦІНА»

У роботі розглянуто принцип комплектування технічними засобами організаційно-технічної складової «інформаційна безпека» інтегральної системи безпеки на основі критерію «ефективність – інтегральна ціна». Проведені дослідження показали неможливість формування універсальної системи безпеки для об'єктів різних типів. У той же час, шлях у вибраному напрямку дозволяє однозначно сформувати загальні принципи розробки інтегральних систем безпеки, які базуються на науково обґрунтованих критеріях, що мають загальну природу формування для всіх без винятку систем безпеки.

Ключові слова: *інтегральна ціна, система безпеки, ефективність.*

Вступ

Постановка проблеми. Процес функціонування об'єкту контролю (ОК) невід'ємно пов'язаний із надходженням та обробкою інформаційних потоків, які в загальному розуміння є відповідною інформаційною складовою, що, в свою чергу, є результатом диференціювання внутрішніх процесів в структурі ОК та зовнішніх процесів, по-перше, між суміжними об'єктами, по-друге, між ОК та оточуючим середовищем. У той же час, сучасний розвиток інформаційних взаємовідношень не виключає ризик впливу внутрішніх та зовнішніх небезпек на функціонування ОК (рис. 1).

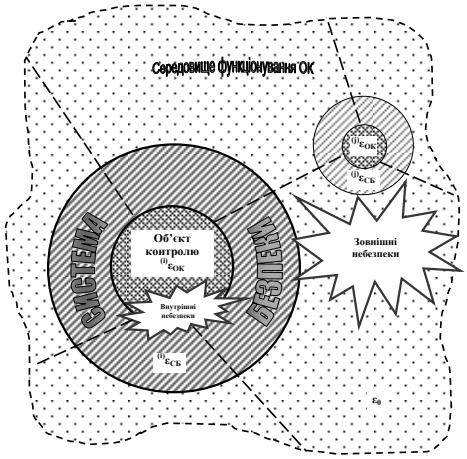

Рис. 1. Умови функціонування системи безпеки (ε_0; $\varepsilon_{ОК}$; $\varepsilon_{СБ}$ – властивості: середовища, в якому функціонує об'єкт; об'єкту контролю (ОК); системи безпеки)

Обмежена ефективність використання можливостей вже існуючих технічних засобів з попередження та усунення інформаційних небезпек ставить перед спеціалістами з розробки систем безпеки ряд економічних, організаційних та технічних проблем пов'язаних з визначенням критеріїв з урахуванням яких повинна формуватися складова «інформаційна безпека» загальної інтегральної системи безпеки ОК.

Аналіз останніх досліджень та публікацій. Загальні питання щодо розробки системи безпеки, як невід'ємної складової функціонування об'єктів різного рівня, розглянуті в [1 – 7]. Так зокрема, розглядаються питання від визначення функцій цієї системи [8], її управління [9] до розробки підсистем отримання [10], передачі [11] та обробки інформації [12, 13]. У той же час чітких критеріїв, які б враховували особливості економічного та технічного розвитку регіону (держави, суспільства), на даний час немає, що зі свого боку породжує питання щодо відповідності (адекватності) заходів з попередження та ліквідації до імовірних втрат в наслідок небезпек.

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

В процесі формування відповідного базового критерію, який є основою для вибору технічних засобів системи безпеки у запропонованому вигляді, необхідно відповісти на ряд питань, які неодноразово піднімались в літературі, а саме: чи повинні втрати на безпеку «об'єкту» сягати щорічно 10% від прибутку; чи достатньо цієї суми для отримання необхідного рівня безпеки, чи навпаки забагато; який повинен бути термін такого фінансування; чи можливо нерівномірне фінансування безпеки (наприклад, на начальному етапі встановити більше фінансування на створення системи безпеки, а потім зменшити обсяг фінансування для підтримки та оновлення системи); як розподілити розміри фінансування між складовими інтегральної системи безпеки; чому слід більше приділити уваги – організаційним заходам або технічним засобам; як вибрати із всього різноманіття технічних засобів представлених на ринку необхідне та інші питання.

Постановка задачі та її вирішення

Метою роботи є по-перше, подальший розгляд та формування організаційно-технічних складових з побудови інтегральної системи безпеки; по-друге, формування критерію «ефективність – інтегральна ціна» як основи принципу комплектування складової «інформаційна безпека» інтегральної системи безпеки технічними засобами. На рис. 1 наведені умови функціонування системи безпеки, що в свою чергу дозволяє сформувати принцип комплексної оцінки небезпек, які впливають на функціонування об'єкту контролю, та розкрити місце даної системи безпеки у постійному процесі запобігання проявам внутрішніх ті зовнішніх небезпек.

Загальна структурна схема системи безпеки технологічних системах (до яких відносяться інформаційні системи) приведена на рис. 2.

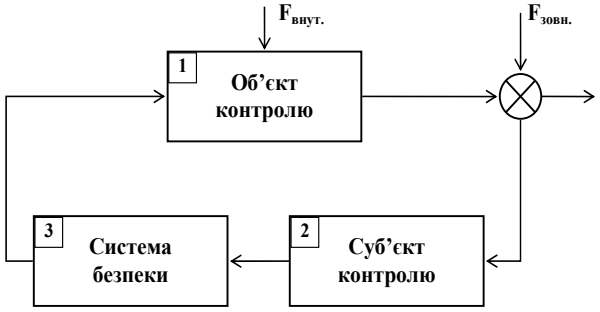

Рис. 2. Структурна схема функціонування системи безпеки ($F_{зовн.}$ – зовнішні небезпеки; $F_{внут.}$ – внутрішні небезпеки)

Узагальнено, інтегральна система безпеки за функціональними признаками є багатокомпонентною системою (рис. 3).

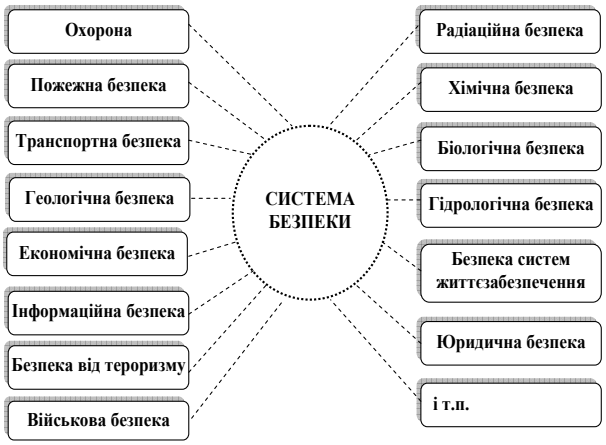

Рис. 3. Структура інтегральної системи безпеки за функціональними признаками

У зв'язку з цим, сума затрат на розбудову такої системи $S^{СБ}$ має вигляд:

$$S^{СБ} \geq U / k_U; \quad 0 < k_U \leq 10 \quad [14, 15];$$

$$S^{СБ} = \sum_i S^{(i)}, \qquad (1)$$

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

Надалі слід визначити наступне припущення: з подальшого розгляду $S^{СБ}$ 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 кількості 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 проявів небезпеки або безпосередня ліквідація небезпеки. 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 проблему про визначення пріоритетів розвитку цих складових, і відповідно проблему щодо розподілу обмеженого (1) економічного потенціалу. Загальний підхід до визначення пріоритетів з техніко-економічного обґрунтування засобів системи безпеки розглянемо на прикладі розбудови складової «інформаційна безпека».

Так, за даними досліджень, проведеними Computer Security Institute та ФБР (CSI/FBI Computer Crime and Security Survey), розмір втрат від небезпеки у інформаційних системах розподілився як на рис. 4 (у опитуванні приймали участь понад 1000 провідних підприємств з розробки та надання інформаційних послуг) [16].

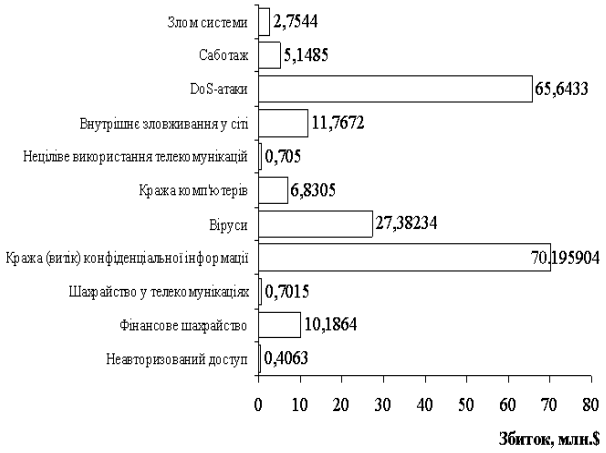

Рис. 4. Розмір збитку підприємств за видами атак на інформацію, що оберталась у процесі їх діяльності у 2003 р. за даними CSI/FBI Computer Crime and Security Survey

Згідно рис. 4 найбільш небезпечними чинниками виступають зовнішні впливання на інформації з метою її знищення або викривлення та несанкціонований доступ до конфіденційної інформації. Умови функціонування системи безпеки з метою попередження та ліквідації даних небезпек представлено на рис. 5 – 6. В межах складової «інформаційна безпека» можливо визначити наступні напрямки заходів її реалізації – рис. 7.

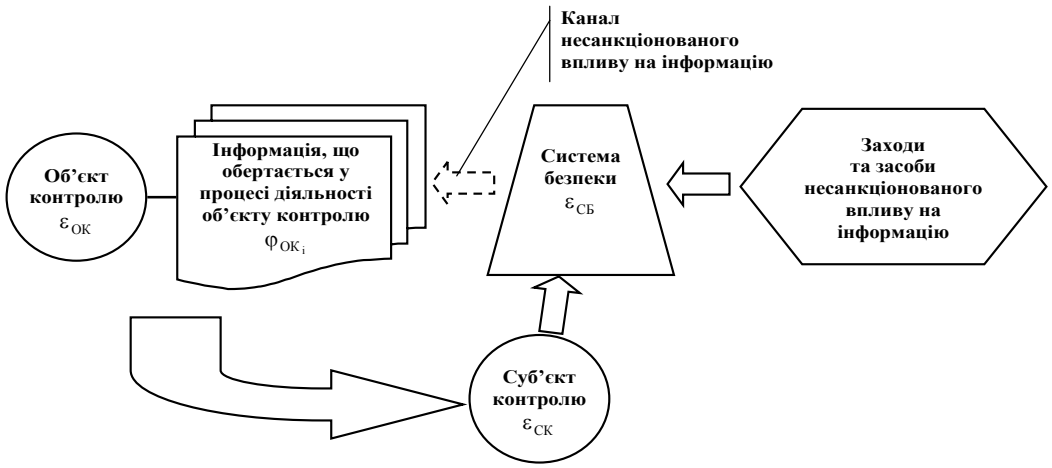

Рис. 5. Схема функціонування елементу „інформаційна безпека" інтегральної системи безпеки з метою недопущення несанкціонованого впливу на інформацію, що обертається у процесі діяльності об'єкту контролю

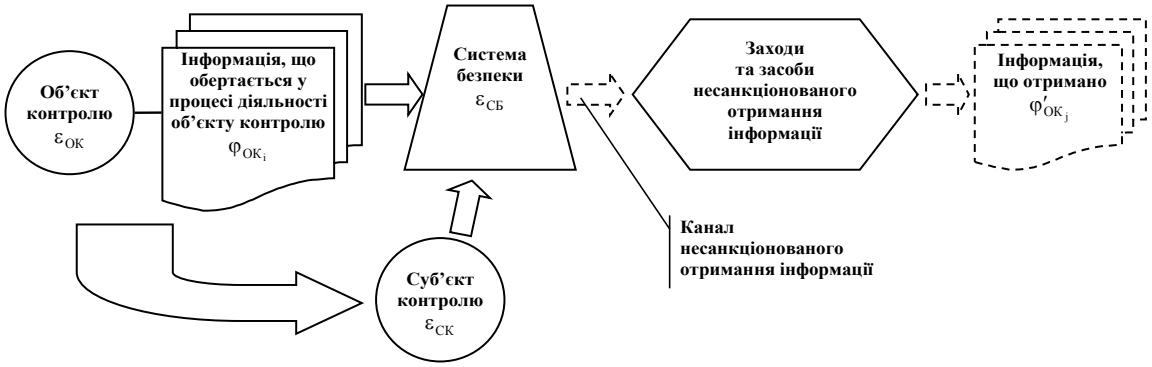

Рис. 6. Схема функціонування елементу „інформаційна безпека" інтегральної системи безпеки з метою недопущення несанкціонованого доступу до інформації, що обертається у процесі діяльності об'єкту контролю

Рис. 7. Структура елементу «інформаційна безпека» інтегральної системи безпеки

Таким чином, затрати на реалізацію даного елементу інтегральної системи безпеки складають:

$$S^{(ІБ)} = S^{(ІБ)}_{орг.} + S^{(ІБ)}_{орг.–тех} + S^{(ІБ)}_{тех}. \qquad (2)$$

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) – табл. 1.

Запропонований підхід розглянемо на прикладі комплектації підсистеми «інформаційна безпека» технічними засобами захисту від несанкціонованого доступу .

Таблиця 1

Вагомість заходів складової «інтегральна безпека» системи безпеки у розподілі економічного потенціалу

Економічний потенціал	Система безпеки
$S^{(ІБ)}_{орг.} \uparrow + S^{(ІБ)}_{орг.–тех} + S^{(ІБ)}_{тех}$	Орієнтована на організаційні заходи
$S^{(ІБ)}_{орг.} + S^{(ІБ)}_{орг.–тех} \uparrow + S^{(ІБ)}_{тех}$	Орієнтована на організаційно-технічні заходи
$S^{(ІБ)}_{орг.} + S^{(ІБ)}_{орг.–тех} + S^{(ІБ)}_{тех} \uparrow$	Орієнтована на технічні заходи
$S^{(ІБ)}_{орг.} \approx S^{(ІБ)}_{орг.–тех} \approx S^{(ІБ)}_{тех}$	Рівно зорієнтована

Відповідно маємо:

$$S^{(ІБ)}_{техн.} = S^{(ІБ)}_{т_1} + S^{(ІБ)}_{т_2} + S^{(ІБ)}_{т_3}, \qquad (3)$$

де $S^{(ІБ)}_{т_1}$, $S^{(ІБ)}_{т_2}$, $S^{(ІБ)}_{т_3}$ – складові цін засобів попередження небезпеки, які обумовлені: властивостями каналів несанкціонованого доступу до інформації (рис. 8); вибором типу технічного засобу (рис. 9); технічними характеристиками відповідно.

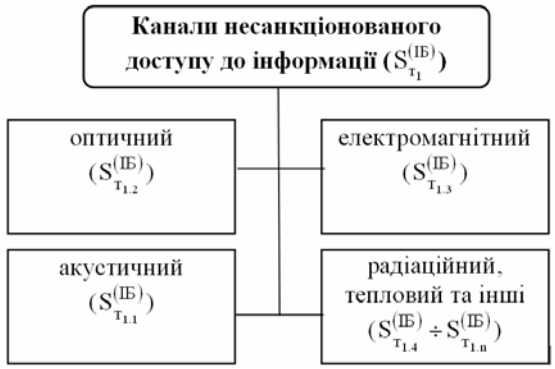

Рис. 8. Загальна структура каналів несанкціонованого доступу до інформації

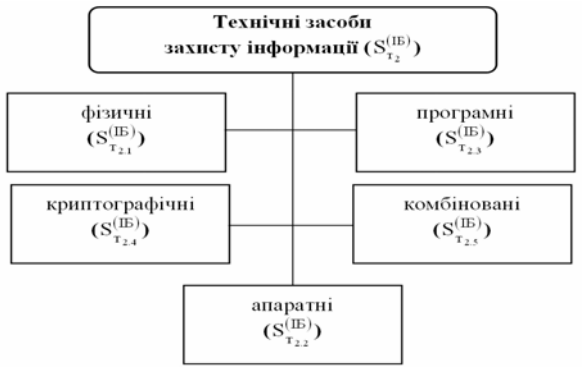

Рис. 9. Загальна структура технічних засобів з захисту інформації від несанкціонованого доступу

Апаратні засоби з захисту інформації від несанкціонованого доступу об'єднують технічні засоби, які за принципом роботи, будовою та можливостями виявляють канали витоку 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 ОК, на наявність можливих каналів витоку інформації; виявлення каналів витоку інформації на різного роду об'єктах та у приміщеннях, які входять у структуру ОК; локалізація каналів витоку інформації; пошук та виявлення засобів витоку інформації; протидія несанкціонованому доступу до джерела інформації, що захищається.

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. 10).

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 $S^{(ІБ)}_{т_2}$ 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. 7), комплектації технічними засобами складової «інформаційна безпека» загальної системи безпеки ОК, який необхідно захистити, за критерієм «ефективність – інтегральна ціна». Використовуючи дані, опубліковані в науковій літературі, офіційну інформацію відомих у даному напрямку виробників та інформацію, отриману в рамках роботи виставкових форумів («Технології захисту – 2005», «Технології захисту – 2007», «Зброя та безпека – 2007», «Технології захисту – 2008», «Зброя та безпека – 2008») [17 – 21], за наведеним критерієм проведено аналіз апаратних засобів виявлення радіо каналу несанкціонованого доступу до інформації. Результати представлено у табл. 2 – 4 та узагальнено на рис. 11, 12.

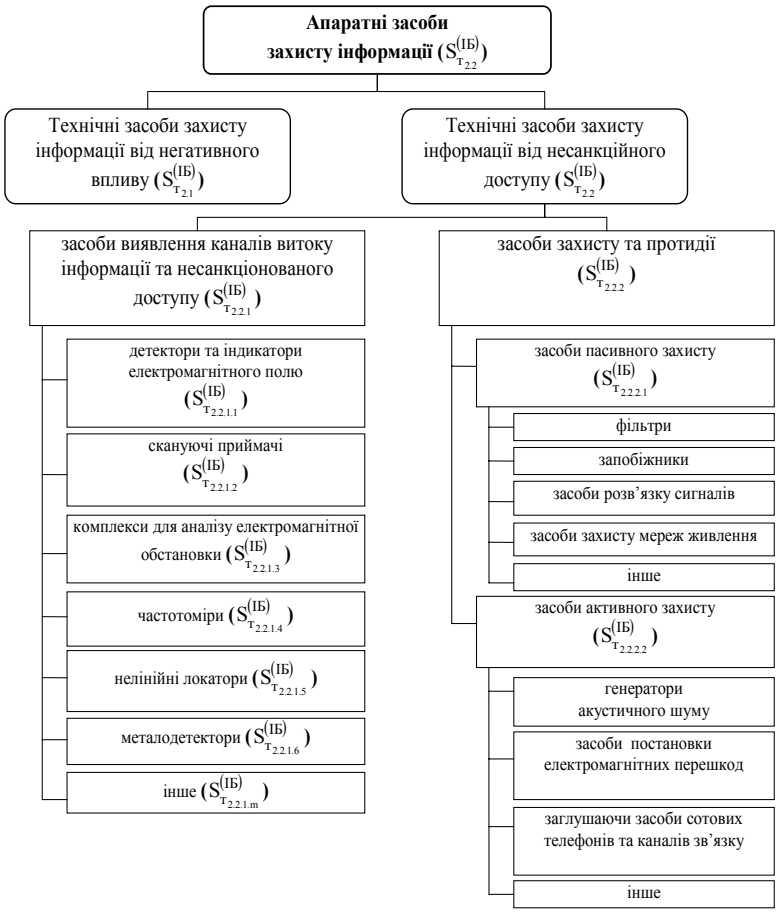

Рис. 10. Загальна структура технічних засобів з захисту інформації

Таблиця 2

Засоби виявлення каналів витоку інформації. Характеристики детекторів та індикаторів електромагнітного полю

Найменування приладу	Пріоритетна характеристика (робочий діапазон, МГц)	Ціна	
		кількісна, у.о.	якісна
RD-11	100 ÷ 6000	144	$S_{т_{1.3}}^{(ІБ)} + \overline{S}_{т_{2.2.1.1}}^{(ІБ)} + \overline{S}_{т_3}^{(ІБ)}$
PROTECT 1203	10 ÷ 3600	210	
«Зажигалка»	54 ÷ 7200	278	
PROTECT 1205	30 ÷ 2400	286	
PROTECT 1206	50 ÷ 3600	490	
• • •			

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

Таблиця 3

Засоби виявлення каналів витоку інформації. Характеристики скануючих приймачів

Найменування приладу	Пріоритетні характеристики			Ціна	
	робочий діапазон, МГц	чутливість, мкВ	тип модуляції	кількісна, у.о.	якісна
переносні					
IC-R5	10 ÷ 1310	–	NFM, WFM, AM	316	$S_{т_{1.3}}^{(ІБ)} + \overline{S}_{т_{2.2.1.2}}^{(ІБ)} + \overline{S}_{т_3}^{(ІБ)}$
AR-8200 MK3	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 4

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

Найменування приладу	Пріоритетні характеристики			Ціна	
	обочий діапазон, МГ	чутливість, мкВ	видкість обзору, МГц/	кількісна, у.о.	якісна
Спектр–МК	40 ÷ 3000	не гірше 2	до 100	18945	$S_{т_{1.3}}^{(ІБ)} + \overline{S}_{т_{2.2.1.3}}^{(ІБ)} + \overline{S}_{т_3}^{(ІБ)}$
С2М "Квадрат"	40 ÷ 6000	не гірше 2	до 100	19336	
Омега	2000 ÷ 18000	не гірше 2	до 350	23047	
• • •					

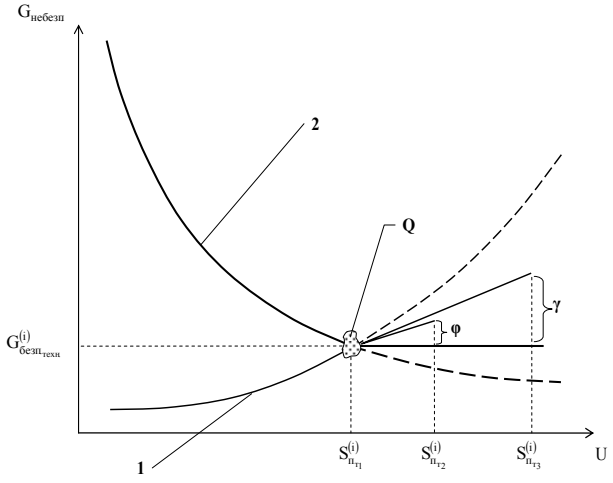

Рис. 11. Залежність рівня безпеки від вибору технічних засобів виявлення і-го каналу несанкціонованого доступу до інформації ($G_{небезп.}$ – рівень небезпеки; U – розмір втрат; $G_{безп.техн.}^{(i)}$ – рівень безпеки, який досягається за допомогою вибраного типу технічного засобу

На рис. 11: 1 – крива, яка характеризую динаміку пріоритетної характеристики і-го каналу несанкціонованого доступу до інформації; 2 – пріоритетна характеристика технічного засобу виявлення і-го каналу несанкціонованого доступу до інформації (сімейство кривих); Q – область функціонування вибраного технічного засобу виявлення і-го каналу несанкціонованого доступу до інформації; φ – приріст рівня небезпеки за умов врахування додаткових необхідних технічних вимог (надійність, періодичність роботи та інше); γ – приріст рівня небезпеки за умов врахування додаткових показників небезпеки заходів та засобів несанкціонованого отримання інформації.

Узагальнення процедури застосування наведеного критерію дає змогу визначити наступний алгоритм дій щодо формування технічної бази інтегральної системи безпеки об'єкту:

1) провести аналіз можливого спектру небезпек, які мають місце у разі виникнення надзвичайної події даного типу;

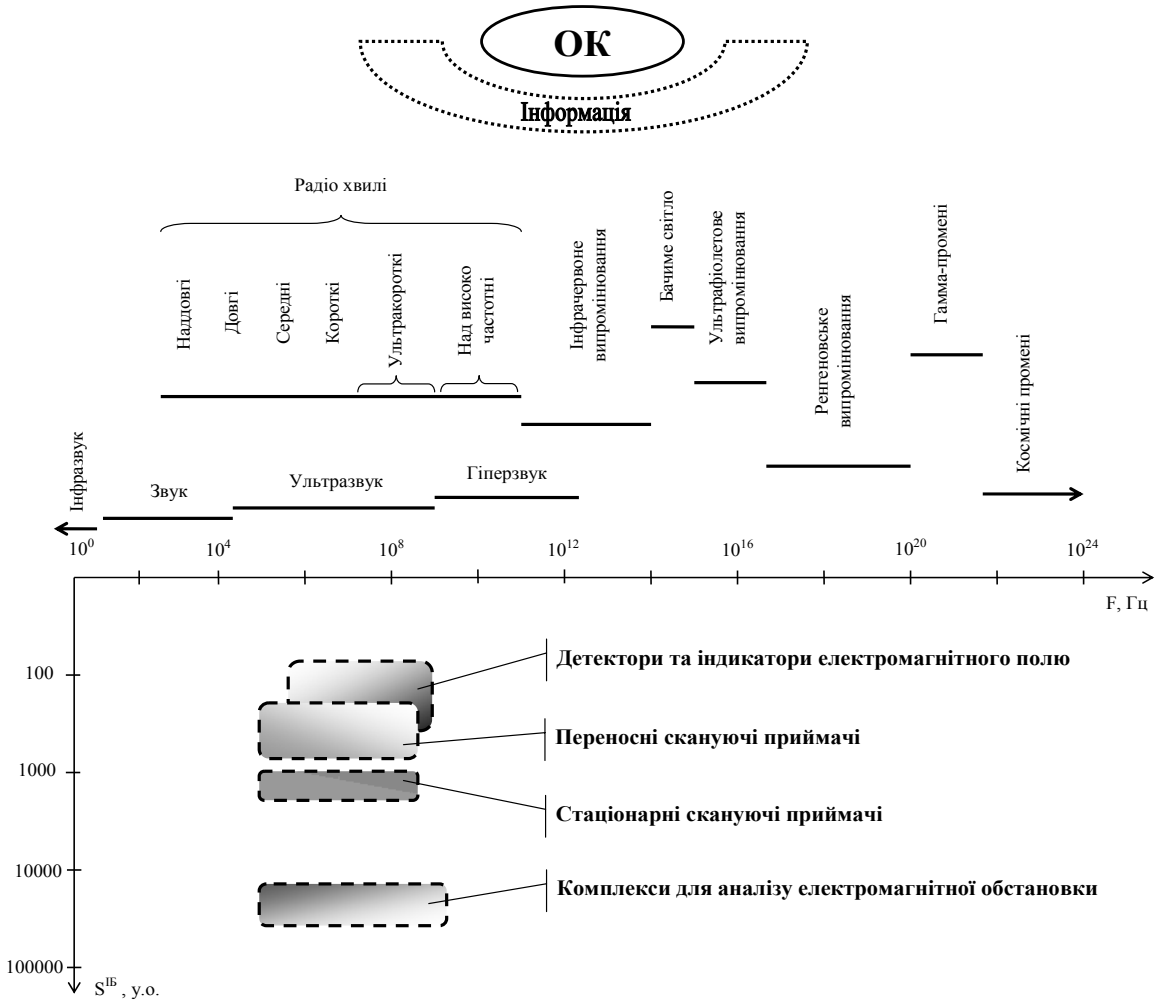

Рис. 12. Графічне представлення областей функціонування технічних засобів виявлення витоку інформації по електромагнітному каналу несанкціонованого доступу в залежності від пропускної частоти каналу (F)

2) сформувати графічну (або аналітичну) залежність між фактором небезпеки (спектром) та пріоритетними характеристиками наявних технічних засобів (рис. 11) в одиницях «безпека – втрати»;

3) виходячи з вимог безпеки об'єкту контролю, визначити пріоритетний фактор небезпеки, що і обумовлює утворення складової «інтегральна ціна» ($S^{(i)}_{п_{т_1}}$) – рис. 8;

4) складові $S^{(i)}_{п_{т_2}}$ та $S^{(i)}_{п_{т_3}}$ визначаються з вимог напрямку діяльності ОК та додаткових вимог, що мають місце на об'єкті (рис. 11, 12).

Висновки

1. Проведені дослідження показали неможливість формування універсальної системи безпеки для об'єктів різних типів. У той же час, шлях у вибраному напрямку дозволяє однозначно сформувати загальні принципи розробки інтегральних систем безпеки, які базуються на науково обгрунтованих критеріях, що мають загальну природу формування для всіх без винятку систем безпеки.

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

3. Використання критерію «ефективність – інтегральна ціна» при формуванні алгоритму комплектування технічними засобами на прикладі засобів інформаційної безпеки (рис. 11, 12) не суперечить отриманим результатам багаторічної практики формування ринку даними технічними засобами безпе-

ки [18 – 21], що дозволяє стверджувати про правильність вибраних підходів та у подальшому застосувати їх при формуванні інших технічних складових інтегральної системи безпеки.

Список літератури

1. Омельчук А.М. Интеграция систем безопасности и нелинейность матрицы угроз / А.М. Омельчук // Системы безопасности. – 2001. – № 41 (октябрь-ноябрь). – С. 20-21.

2. Репин В.И. Интеллектуальное здание. Проблемы и решения / В.И. Репин // Стройпрофиль. – 2001. – № 9. [Электронный ресурс]. – Режим доступа к ресурсу: www.ista.ru.

3. Бояринцев А.В. Анализ уязвимости объектов. Место и роль в создании, модернизации и оценке эффективности систем обеспечения безопасности / А.В. Бояринцев, Н.И. Шумилов // Системы безопасности. – № 42 (декабрь 2001 – январь 2002). – С. 42-43.

4. Мусиенко Д. Экспертиза безопасности объекта / Д. Мусиенко // Бизнес и безопасность. – 2006. – № 6. – С. 3-5.

5. Кондратьев В.Д. Комплексная оценка уровня риска опасного объекта / В.Д. Кондратьев, А.В. Толстых, Б.К. Уандыков, А.В. Щепкин // Системы управления и информац. технологии. – 2004. – № 3 (15). – С. 53-57.

6. Абрамов Ю.О. Моніторинг надзвичайних ситуацій / Ю.О. Абрамов, Є.М. Грінченко, О.Ю. Кірочкін та ін. – Х.: АЦЗУ, 2005. – 530 с.

7. Ярочкин В.И. Система безопасности фирмы / В.И. Ярочкин. – М.: Ось-89, 2003. – 352 с.

8. Абрамов Ю.А. Основные требования к созданию единой системы мониторинга чрезвычайных ситуаций / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Системи обробки інформації. – Х.: Харк. універ. Повітряних Сил, 2005. – Вип. 6 (46). – С. 203-207.

9. Абрамов Ю.А. Основы мониторинга и управления в условиях чрезвычайных ситуаций / Ю.А. Абрамов, В.Е. Росоха, В.В. Тютюник, В.Н. Чучковский, Р.И. Шевченко. – Х.: Изд. АГЗУ, 2005. – 257 с.

10. Палий А.И. Радиоэлектронная борьба / А.И. Палий. – М., 1989. – 349 с.

11. Мухин В.И. Средства информационной борьбы / В.И. Мухин, Ю.И. Набока, В.К. Новиков // Вопросы защиты информации. – 2000. – № 2. – С. 10.

12. Серебровский А.Н. Об оценках ситуаций по потенциально опасных объектах на этапе превентивного мониторинга / А.Н. Серебровский // Мат. машини і системи. – 2000. – № 1. – С. 57-64.

13. Абрамов Ю.А. Информационное обеспечение мониторинга и антикризисного управления в условиях чрезвычайных ситуаций / Ю.А. Абрамов, Е.Н. Гринченко, А.Ю. Кирочкин и др. – Х.: Изд-во УГЗУ, 2006. – 288 с.

14. Шепитько Г.Е. Прогноз рентабельности системы комплексной безопасности предприятия / Г.Е. Шепитько, Г.Н. Гудов, И.И. Медведев // Системы безопасности – 2003. Материалы XII науч.-техн. конф. – Москва, 2003. – С. 82-85.

15. Карпычев В.Ю. Основные экономические подходы к созданию систем безопасности / В.Ю. Карпычев, В.А. Кузнецов // Системы безопасности – 2004. Материалы XIII науч.-техн. конф. – Москва, 2004. – С. 126-128.

16. [Електронний ресурс]. – Режим доступу до ресурсу: www.secretssaver.com/news/news1.html.

17. Черешкин Д.С. Оценка эффективности систем защиты информационных ресурсов / Д.С. Черешкин, В.А. Гадасин, О.И. Елизаров и др. – М.: Ин-тут системного анализа РАН, 1998.

18. Інформаційні ресурси [Електронний ресурс]. – Режим доступу до ресурсів: www.das.kiev.ua; www.klad.com.ua; www.bezpeka.com; www.magazine.security.com.ua; www.security-info.com.ua; www.securpress.ru; www.kiev-security.org.ua; www.opta. com.ua; www.arsenal-sb.ru.

19. Офіційний каталог IV Міжнародного виставкового форуму «Технології захисту – 2005». – К., 2005. – 166 с.

20. Офіційний каталог VI Міжнародного виставкового форуму «Технології захисту – 2007». – К., 2007. – 142 с.

21. Офіційний каталог VII Міжнародного виставкового форуму «Технології захисту – 2008». – К., 2008. – 132 с.

Надійшла до редколегії 9.04.2009

Рецензент: канд. техн. наук, доцент М.І. Адаменко, Харківська державна академія фізичної культури, Харків.

ПРИНЦИП КОМПЛЕКТОВАНИЯ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ СОСТАВЛЯЮЩЕЙ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ИНТЕГРАЛЬНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ПО КРИТЕРИЮ «ЭФФЕКТИВНОСТЬ – ИНТЕГРАЛЬНАЯ ЦЕНА»

В.В. Тютюник, Р.И. Шевченко

В работе рассмотрен принцип комплектования техническими средствами организационно технической составляющей «информационная безопасность» интегральной системы безопасности на основе критерия «эффективность – интегральная цена». Проведенные исследования показали невозможность формирования универсальной системы безопасности для объектов разных типов. В то же время, путь в выбранном направлении позволяет однозначно сформировать общие принципы разработки интегральных систем безопасности, которые базируются на научно обоснованных критериях, которые имеют общую природу формирования для всех без исключения систем безопасности.

Ключевые слова: *интегральная цена, система безопасности, эффективность.*

PRINCIPLE OF COMPLETING HARDWARES OF CONSTITUENT «INFORMATIVE SAFETY» OF INTEGRAL SYSTEM OF SAFETY ON CRITERION «EFFICIENCY is INTEGRAL PRICE»

V.V. Tyutyunik, R.I. Shevchenko

In work principle of completing hardwares is considered organizationally by a technical constituent «informative safety» of the integral system of safety on the basis of criterion «efficiency is an integral price». The conducted researches showed impossibility of forming of the universal system of safety for the objects of different types. At the same time, a way in the chosen direction allows simply to form general principles of development of the integral systems of safety, which are based on the scientifically grounded criteria which have general nature of forming for all without the exception of the systems of safety.

Keywords: *integral price, system of safety, efficiency.*