УДК 621.391

О.Г. Пузиренко[1],О.Ю. Іохов[2],О.М. Горбов[2], І.В. Кузьминич[2]

[1] *Генеральний штаб Збройних Сил України, Київ*
[2] *Академія внутрішніх військ МВС України, Харків*

МЕТОДИКА КІЛЬКІСНО-ЯКІСНОГО АНАЛІЗУ ТА ВИЗНАЧЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті одержано достатньо чіткий критерій визначення характеру інформаційної небезпеки, який виходить із чисельних значень індексу інформаційної небезпеки. За допомогою цього критерію стало можливо уточнювати і рівні стабільності у суспільстві у випадках, коли сукупність значень величин коефіцієнту проникнення та співвідношення сторін суттєво відрізняються від відомих.

***Ключові слова**: індекс інформаційної безпеки, рівень стабільності у суспільстві, коефіцієнт проникнення, імовірність відвернення.*

Вступ

Історія людської цивілізації – це історія воєн як найпотужніших засобів перерозподілу цінностей, територій та здобуття контролю над ними.

За основними об'єктам, що піддаються загрозам, історики виділяють три хвилі воєн: аграрна, індустріальна та інформаційна, вважаючи, що десять століть назад агресор захоплював територію, сто років тому – вражав промисловість, а в даний час повинен паралізувати управління для досягнення своєї переваги.

Інформаційна війна не є надбанням сьогоднішнього дня. Багато прийомів інформаційного впливу виникли тисячі років тому разом з появою інформаційних самонавчальних систем – історія навчання людства це і є свого роду інформаційні війни. При цьому цілком природно, що з підвищенням можливостей інформаційних систем у частині їх навчання, акцент все більше і більше зміщуватиметься у бік застосування не вогнепальної зброї, а інформаційної.

Існування і розвиток сучасних держав відбувається в тісному зв'язку з геополітичними та геостратегічними умовами і значною мірою залежить від рівня інформаційної безпеки в державі.

Вирішення проблеми забезпечення інформаційної безпеки неможливе без постійного аналізу відносин у суспільстві (ВС), районі, державі, світі, виявлення (прогнозування) на цій основі інформаційної безпеки, що існує або може виникнути, та вжиття адекватних заходів щодо її реалізації.

Відомо, що відносини у суспільстві – це конкретний стан відносин у суспільстві, регіоні, партій, соціальних груп, пов'язаний зі створенням використанням можливостей відвернення атак [1]. Оцінка ВС має характер науково-теоретичного пізнання і опирається на такі методологічні принципи [2]:

– об'єктивність та реалістичність;
– всебічність та комплексність аналізу;
– конкретний підхід.

Однак реалізація цих принципів потребує обґрунтованих методичних підходів і прийомів для визначення дійсних справ, фактичного співвідношення сил, тенденцій розвитку подій, за якими стоять певні інтереси, можливості та дії.

Зараз у науковому світі активізувалася робота по оцінці рівня інформаційної безпеки із застосуванням математичних методів [1 – 4]. Проте існуючі моделі і методи, доступні з відкритого друку, далекі від досконалості.

Таким чином, до цього часу не існує адекватної методики оцінки як кількісного, так і якісного рівня інформаційної безпеки.

Основними проблемами, які необхідно розв'язати для розробки методичних основ кількісно-якісного аналізу ситуаційної обстановки та визначення рівня інформаційної безпеки є:

визначення функціональної залежності між кількісними значеннями часткових показників суспільної обстановки та індексом інформаційної безпеки;

розробка критерію оцінки рівня інформаційної безпеки, виходячи з усієї сукупності її якісних та кількісних характеристик;

визначення методики обґрунтування пріоритетних заходів, спрямованих на забезпечення належного рівня інформаційної безпеки.

Мета досліджень – створення методики кількісно-якісного аналізу і визначення рівня інформаційної безпеки.

Постановка завдання. У зв'язку з цим основне завдання полягає у розробці методичних основ оцінки рівня інформаційної безпеки, залежно від існуючих і потенційних загроз та обґрунтування рекомендацій щодо удосконалення механізму захисту інтересів об'єкту в інформаційній сфері.

Формалізоване поставлення задачі дослідження можна визначити як пошук та вивчення залежності

$$Y = f(x_1, x_2, \ldots, x_k), \qquad (1)$$

де Y – цільова функція об'єкта дослідження,

$x_1,x_2,\ldots,x_k$ – чинники, які суттєво впливають на стан об'єкта дослідження,

k – загальна кількість чинників, що розглядаються.

Залежність (1) пов'язує цільову функцію з основними чинниками, які впливають на її значення, тобто є математичною моделлю об'єкта досліджень. Кожен з фіксованих наборів чинників визначає конкретне значення цільової функції. Таким чином, пошук раціональних шляхів забезпечення інформаційної безпеки полягає у визначенні такої сукупності $x_1,x_2,\ldots,x_k$, яка забезпечує наближене до максимального значення цільової функції Y за умови існуючих обмежень.

Як вже було визначено у [3], такою цільовою функцією може бути індекс інформаційної безпеки. Способи визначення величин, які визначені у [3] для обчислення індексу інформаційної безпеки, можуть бути різними. Найпростішим шляхом є проведення експертних опитувань, але більш ґрунтовні і достовірні оцінки можуть бути отримані за допомогою функціональної залежності індексу інформаційної безпеки від об'єктивних кількісних характеристик суспільної обстановки та інших факторів, що впливають на інформаційну безпеку.

Першим кроком до розвитку індексу інформаційної безпеки має бути визначення індексу інформаційної небезпеки як імовірнісні заподіяння суттєвої шкоди інформації, яка є власністю підприємства, організації, держави або власника. Така імовірність має у своїй основі імовірність самої атаки. У свою чергу, атаку на інформацію можна ототожнити з прийняттям порушником або зловмисником – ініціатором атаки рішення про атаку. Важливу роль у визначенні індексу інформаційної небезпеки відіграє врахування можливостей носія інформації та самої інформації – об'єкта потенційної атаки щодо її отримування та відбиття.

Таким чином, опираючись на міркування, наведенні у [3], розрахунок індексу інформаційної небезпеки у взаємовідносинах двох суб'єктів (назвемо їх сторонами А і В) можна звести до визначення імовірності прийняття потенційного порушника або зловмисника (нехай ним буде сторона А) рішення про здійснення атаки того чи іншого масштабу проти сторони В та імовірності успіху атаки за умов конкретних можливостей сторони В щодо її відбиття або відвернення.

З урахуванням досліджень проведених у [3] та підходу до кількісно-якісної оцінки суспільної

ситуації наявного об'єкту, головними висновками з такої оцінки можуть бути:

співвідношення "виграш-програш" для сторони А, тобто величина K_{ex}^{ab};

співвідношення сил сторін, тобто величина G^{ab}.

На підставі цих висновків, а також під впливом інших об'єктивних та суб'єктивних факторів рішення сторони А про початок атаки на інформацію сторони В може бути прийняте або не прийняте. Певний вплив на це рішення буде чинити, зокрема рівень підготовки та готовністю сторони А до позитивного сприйняття такого кроку стосовно сторони В.

Таким чином, рішення про атаку слід вважати подією, імовірність настання якої на прогнозований час визначається, головним чином, переліченими раніше факторами і умовами. Цю імовірність можна ототожнити з імовірністю атаки, яку в [3] позначено через $P_{АТАК}$. Оскільки здійснення атаки та її відвернення згідно з [3] випливає, що

$$P_{АТАК} = 1 - P_{відв} = (1-P_{пас})(1-P_{акт}), \qquad (2)$$

де $P_{АТАК}$ – імовірність протидії атаки на інформацію; $P_{відв}$ – імовірність відвернення атаки на інформацію; $P_{пас}$ – імовірність пасивного відвернення атаки на інформацію; $P_{акт}$ – імовірність активного відвернення атаки на інформацію.

Розгляд рівняння (2) з точки зору залежності співмножників, що входять до його правої частини, від перелічених раніше показників соціальної обстановки, приводить до таких висновків:

По-перше, відвернення атаки зводиться по суті, до зменшення величини, тобто до наближення, наскільки це можливо до балансу інтересів сторін А і В. Досягнення цієї мети сприятиме також і збільшення всіма можливими шляхами і засобами прогнозованої величини L^{AB} . Загальним результатом буде зменшення коефіцієнта проникнення $K_{про}^{AB}$.

Крім того слід враховувати, що

$$K^{AB}_{про}=V^{AB}/ L^{AB},$$

де V^{AB} – виграш сторони А;

L^{AB} – збиток, який зазнає сторона А в ході атаки на інформацію сторони В;

По-друге, активне відвернення можливої атаки, так само як і її відбиття, досягається головним чином, шляхом забезпечення відповідного співвідношення сил з урахуванням очікування атаки.

Таким чином, між значеннями $K_{про}$ і G (під час подальших досліджень індекси А і В для спрощення запису будуть випущені) та імовірністю $P_{АТАК}$ існує пряма залежність. Очевидно, що зростання величин $K_{про}$ і G веде до зростання величин $P_{АТАК}$ і навпаки. Проте ні характер цієї залежності, ні тим більше функціональний зв'язок між зазначеними показниками і величиною $P_{АТАК}$ невідомі.

Для вирішення шляхів вирішення поставлених питань доцільно звернутися до теорії прийняття рішень [4, 5].

Відповідно до [4], у разі задач з ризиком особа, яка приймає рішення (ОПР), створює власне евристичне уявлення про задачу як список факторів (вимірів), що включає величину виграшу, величину програшу, імовірність програшу та рівень ризику. Рі-

шення, за твердженням [4], є функцією двох основних змінних величин: величини виграшу (ВВ) та ризику (R). У результаті проведених досліджень установлено, що під час оцінювання ризику беруть до уваги, головним чином, величину програшу (ВП) та суб'єктивну імовірність програшу (СІП). Для умов, визначених в [4, 5] досліджень емпірична залежність для оцінки величин ризику визначається рівнянням

$$R = 3{,}12(\text{СІП}) + \lg(\text{ВП}). \qquad (3)$$

За твердженням [4] та [5], формула (3) має велику прогностичну цінність. Коефіцієнт кореляції між оцінками, отриманими за допомогою (3), та оцінки авторів склала біля 0,98, що свідчить про високу точність прогнозу. Відповідь на запитання про те, як сполучення величин виграшу ВВ та ризику R впливає на відсоток, який приймає запропоновані умови виграшу та ступінь ризику, дає рівняння регресії за [5]:

$$Д\ (\%) = 1{,}45(\text{ВВ}) - 49{,}1(R) + 140, \qquad (4)$$

яке отримано за підсумками проведених досліджень. При цьому коефіцієнт кореляції між оцінками, одержаних за допомогою (4) та даними досліджень, склав 0,9, що також є доказом високої збіжності. Віддаючи належне коректності результатів, одержаних [4, 5], слід у той самий час зауважити, що в інтересах даного дослідження ці результати не можуть бути використані без застережень. Справа в тому, що умови проведення описаних в [4, 5] експериментів, які полягали в пред'явленні їх учасником альтернатив у вигляді виграшу у сполученні з певним ризиком програшу, не можна співставляти з умовами прийняття найважливіших рішень зловмисником. Крім того, в сфері інформаційних відносин виграш або програш (збиток) далеко не завжди може мати пряме матеріальне або грошове обчислення.

Однак у теорії прийняття рішень уважається практично загальновизнаним той факт, що фундаментальні закони, які визначають процес оцінки альтернатив, не зазнають модифікації під впливом змінювання цілей ОПР. Модифікація структури цілей може спричинити кількісні, але не якісні зміни [5]. Тому загальний характер екстримально встановлених залежностей між значеннями можливого виграшу і ступеня ризику, з одного боку, та імовірністю прийняття ОПР таких умов, з іншого боку, можна екстраполювати і на умови задачі, яка розглядається.

Використання виявлених у [4, 5] закономірностей для вирішення поставлених у даному дослідженні завдань може бути аргументовано ще й таким чином: на рівні буденної свідомості висновки [4] можна вважати адекватними.

Розглянуті результати досліджень у галузі теорії прийняття рішень, у сукупності із запропонованими у [3] підходом до визначення чисельних значень показників інформаційної небезпеки і інформаційної безпеки, можуть бути основою для визначення функціональної залежності між імовірністю початку атаки і такими показниками відношеннями в суспільстві як коефіцієнт проникнення $K_{про}$ та співвідношення сил, тобто залежності

$$P_{АТАК} = f\,(K_{про}, G). \qquad (5)$$

Вихідні положення для вирішення цього завдання можна сформулювати таким чином:

1. Стосовно термінології, прийнятої в [3 – 5], для дослідження стратегій вибору під час вирішення задач з ризиком, можна провести аналогії між такими поняттями:

величиною виграшу ВВ та відносним виграшем V;

величиною програшу ВП та відносним програшем L;

значенням суб'єктивної імовірності програшу СІП та величиною співвідношення сил Q (оскільки саме співвідношення сил найбільшою мірою визначає імовірність успіху або провалу атаки).

2. Функція (5) є монотонно зростаючою і обмеженою знизу значенням, що дорівнює нулю, зверху значенням, що дорівнює одиниці. При цьому швидкість зростання функції (5) до максимального значення залежить, головним чином, від величини G.

3. В області малих значень $K_{про}$ крива (5) полого зростає. Також полого вона зростає, асимптотично наближаючись до верхньої межі, при великих значеннях $K_{про}$. В області середніх значень $K_{про}$ слід очікувати на точку перетину функції (5) як наслідок зміни швидкості її зростання.

4. Існує характерне значення $P_{АТАК} = 0{,}25$ при $K_{про} = 1$, $G = 1$. Це твердження може бути

аргументовано таким чином: якщо $K_{про} = 1$, то це означає рівноймовірність позитивного і

негативного результатів спроб пасивного урегулювання ситуації, тобто у рівнянні (2) можна

вважати $P_{пас} = 0{,}5$; при G=1 жодна із сторін не має переваги у сфері протистояння, тобто у рівнянні (2) можна вважати $P_{акт} = 0{,}5$. Отже, прийняте вище припущення є достатньо

обґрунтованим, оскільки воно безпосередньо витікає з (2).

Слід припустити, що за фіксованих значень $K_{про}$ існує певна залежність $P_{АТАК}$ від абсолютних значень V і L, яка виявляється у зростанні $P_{АТАК}$ при переміщенні величин V і L в область мінімальних або максимальних значень.

Викладені вихідні дані у зіставленні з результатами вивчення досвіду математичного моделювання та прогнозування різноманітних інформаційних і технічних процесів приводить до висновку, що умовам даної задачі найбільшою мірою відповідає математична залежність, яка одержала широке та підтверджене експериментальним шляхом застосування для кількісного прогнозування у багатьох областях знань [4, 5]. $1+ae^{-bt}$

Ця залежність визначається [5] формулою:

$$U=F/1+ae^{-bt}, \quad (6)$$

де U – значення шуканої величини залежно від значення змінної величини t; F – верхня межа росту величини U; t – змінна величина (аргумент); e – основа натуральних логарифмів; a – безрозмірна константа; b – константа, що має розмірність 1/t.

З урахуванням прийнятих позначень ($K_{про}$ є аналогом змінної величини t), рівняння (6) набуває такого вигляду:

$$P_{АТАК} = 1/1+ae^{-bk\ про}. \quad (7)$$

Для уточнення залежності (7) необхідно визначити, стосовно даної задачі, величини “a” і ”b”.

Тому слід прийняти b=G, тобто чим більше G, тим, отже, менше ступінь ризику і тим більш круто піде крива (7) є механізмом взаємокомпенсації величини ризику і величини виграшу, що має важливе значення у теорії прийняття рішень [5].

Для виявлення смислового значення величини “a” звернемо увагу на таке.

Очевидно, що при $K_{про} = 0$ і/або G=0

$$P_{АТАК} =1/1+a, \quad (8)$$

але оскільки також очевидно, що величина $P_{АТАК}$ дорівнює за цих умов нулю, слід визначити, що величина “a” повинна мати нескінченно велике значення. Отже, рівняння (7) начебто втрачає свій смисл.

Тому може бути цілком логічним висновок про те, що за умови даної задачі величина “a” не є константою. Вона залежить від $K_{про}$ та G і при $K_{про} \rightarrow 0$ та/або $G \rightarrow 0$ набуває такого значення, яке наближається до нескінченно великої величини. Отже, величина “a” має бути обернено пропорційною величинам $K_{про}$ і G. Іншою мовою, яку має задовольнити величина “a”, є виконання рівності АТАК P =0,25 при $K_{про}$ =1, G=1. За допомогою формули (7) легко переконатися, що цій умові відповідає значення a = 3e = 8,15.

Таким чином, стосовно даної задачі величина “a” не може бути константою. Її значення пов’язане з величинами $K_{про}$ і G залежністю

$$a = 3e/ K_{про} G. \quad (9)$$

Отже, функціональна залежність (7) може бути подана рівнянням:

$$P_{АТАК} = 1/1+ 3e/ K_{про} G. \quad (10)$$

1 етап. Розглянемо залежність (10) стосовно прийнятої у [3] класифікації характеру відносин у суспільстві. Баланс інтересів, який характеризується близькими до нуля значеннями $K_{про}$ і визначає стабільність на основі балансу інтересів, має головною особливістю відсутність вираженої інформаційної небезпеки незалежно від наявності або відсутності балансу сил.

Стабільність на основі балансу сил, коли $0< K_{про} <1$, є менш стійким станом, який характеризується наявністю потенційної інформаційної небезпеки. При цьому величина $P_{АТАК}$ може досягати значення 0,25. Не можна не звернути уваги і на таке питання, як рівень ефективності системи захисту та технічних можливостей зловмисника, відповідно до якого досягнуто балансу сил. Чим більше цей рівень, тим більшими або абсолютною величиною можуть бути значення V, а це, у свою чергу, зменшує величину “a” і через веде до зростання $P_{АТАК}$.

Таким чином, навіть за наявності балансу сил зростання рівня технічних можливостей сторін об’єктивно підвищує імовірності можливості атаки на інформацію.

З іншого боку, при не зменшенні величини V зростання технічних можливостей сторін об’єктивно збільшує значення L, а це у свою чергу, зменшує $P_{АТАК}$. Так виявляється стримуючий вплив технічних можливостей сторін з точки зору відвернення атак. І навпаки, зниження рівня технічних можливостей сторін може привести до такого зростання величини $K_{про}$ (через зменшення L), за яким атака може відбутися навіть з незначного приводу (тобто за малих значень V) з відповідним об’єктивним зменшенням масштабу втрати інформації.

Відносна стабільність на основі врегулювання ($0< K_{про} <1$, G>1) хоча і означає деяке зростання інформаційної небезпеки (наприклад, при $K_{про}$ = 0,75 і G=1,5 імовірність здійснення атаки наближається до значення 0,3), однак, це ще може пов’язуватися з потенційною інформаційної небезпеки. Відносна стабільність на основі стримування ($K_{про}$ >1, G = 1) означає зростання інформаційної небезпеки до реальної. На графіках рис. 5 можна бачити, що вже при $K_{про}$ = 1,5, G = 1 імовірність здійснення атаки може досягати значення 0,45. За цих умов порушення балансу сил, тобто перехід величини G в область значень, які суттєво перевершують одиницю, веде до різкого зростання $P_{АТАК}$, що, згідно з прийнятою класифікацією, означає нестабільність на основі дисбалансу сил та інтересів. При цьому таку нестабільність, залежно від величини $P_{АТАК}$ можна пов’язувати з атакою або безпосередньою загрозою інформації.

Таким чином, висновки щодо класифікації, одержані у [3], достатньою мірою узгоджуються з кількісними оцінками імовірності протидії атаки на інформацію, одержані за аналогічних умов за допомогою залежності (10).

2 етап. Оцінку відповідності результатів одержаних із використанням залежності (10), експериментальним даним з області дослідження стратегії вибору при розв’язанні задач з ризиком [4,5,] доцільно провести згідно з тими вихідними позиціями, що були сформульовані під час розробки підходу до визначення функціональної залежності (5).

Вимоги п.п. 1 – 4 виконані повністю, оскільки саме виходячи з них вибрано характер та конкретний вид залежності (10).

Для оцінки виконання вимог п. 5 припустимо, що величина $K_{про}$ зафіксована при деяких середніх значеннях величин V і L. При цьому склалося деяке

співвідношення сил G, що у сукупності визначає відповідне значення $P_{АТАК}$. Пропорційне одночасне зміщення величин V і L в область менших або більших значень без зміни величини $K_{про}$ означає відповідні зміни в менший або більший бік зловмисних цілей потенційного нападника, так і прогнозованих втрат сторін у випадку зловмисних дій. Останні, в свою чергу, значною мірою залежать від рівнів технічного забезпечення сторін. З огляду на це певне зростання в обох випадках величини $P_{АТАК}$ можна пов'язати з дією відмічених у [3] закономірностей щодо впливу рівнів технічної оснащеності сторін на імовірність виникнення зловмисних дій.

Таким чином, на рівні якісної оцінки вимоги п. 5 можна вважати виконаними. Кількісну оцінку цього явища можна дати тільки на основі результатів конкретних розрахунків, тобто на подальших етапах дослідження. Проведений аналіз дає змогу стверджувати, що задача об'єктивної кількісної оцінки імовірності протидії атаки на інформацію однією зі сторін одержала задовільне рішення, яке подане залежністю (10). Наступним кроком на шляху до визначення індексу інформаційної небезпеки є кількісна оцінка імовірності успіху несанкціонованих та зловмисних дій у випадку атаки на інформацію.

Успіх (не відбиття) атаки є подією, протилежною її успішного відбиття. Якщо позначити імовірність не відбиття атаки $P_{нвід}$, то очевидно, що

$$P_{нвід} = 1 - P_{від}. \qquad (11)$$

Таким чином, питання зводиться по суті, до визначення величини $P_{від}$. Рівняння [3]:

$$P_{від} = P_{лок} + P_{від\,(лок)} + P_{рег} + P_{від(рег)} + P_{нац} + P_{від\,(нац.)} + P_{глоб} + P_{від\,(глоб)}, \qquad (12)$$

де $P_{від\,(лок)}$, $P_{від(рег)}$, $P_{від\,(нац.)}$, $P_{від\,(глоб)}$ – імовірності відбиття атаки на інформацію відповідного характеру. Це рівняння для розрахунку $P_{від}$ містить кілька доданків, значення яких залежить від ймовірностей небуття можливої атаки того або іншого масштабу та імовірності її відбиття за відповідних умов.

Порядок визначення масштабу атаки на інформацію розглянуто у [3]. Однак значення цього показника слід розглядати як математичне очікування випадкової величини, що розглядається згідно з деяким законом. Такий висновок ґрунтується на залежності масштабу атак на інформацію від великої кількості випадкових факторів. Саме з тих причин рівняння (12) враховує різні умови відбиття атак.

Проте індекс інформаційної безпеки не має достатньої цінності без зіставлення його з іншими показниками, що характеризують інформаційну безпеку. Ця проблема може бути сформульована як необхідність вибору критерію оцінки рівня інформаційної безпеки за всією сукупністю її основних кількісних та якісних характеристик.

У першу чергу, необхідно пов'язати можливі чисельні значення індексу інформаційної небезпеки з прийнятими рівнями стану відносин у суспільстві стабільності в інформаційному просторі та визначеннями характеру інформаційної небезпеки.

Аналіз порівняльних даних щодо ймовірностей відвернення і протидії атаці, а також відповідних значень індексів інформаційної небезпеки, розрахованих за допомогою формул (9,10) у зіставленні з прийнятими рівнями стабільності та відносин у суспільстві приводить до висновків наведених в табл. 1:

потенційній інформаційній небезпеці відповідають значення індексу інформаційної небезпеки в межах $0 \div 0{,}15$;

стан загрози інформаційної або атака настає при досягненні індексом інформаційної

небезпеки значення, яке дорівнює або більше від 0,5, при цьому безпосередній інформаційної загрози відповідають значення $P_{нб} \geq 0{,}75$;

проміжні значення $0{,}15 < P_{нбі} < 0{,}5$ слід віднести до реальної інформаційної небезпеки.

Таблиця 1

Залежність характеру інформаційної небезпеки від показників стану відносин у суспільстві

Рівень стабільності у суспільстві	Характерні значення кількісних показників відносин у суспільстві			Характер інформаційної небезпеки
	$K_{про}$	G	$P_{нбі}$	
Стабільність на основі балансу сил та інтересів	≈ 0	≈ 1	≈ 0	Відсутність інформаційної небезпеки
Стабільність на основі балансу інтересів	≈ 0	$\neq 1$	≈ 0	
Стабільність на основі балансу сил	Менше 1	≈ 1	До 0,15	Потенційна інформаційна небезпека
Відносна стабільність на основі пасивного відвернення	Менше 1	Більше 1	0, 15 ÷ 0,5	Реальна інформаційна небезпека
Відносна стабільність на основі активного відвернення	Більше 1	Менше 1		
	Більше 1,5	Більше 1,5	0, 5 ÷ 0,75	Інформаційна загроза
Нестабільність на основі дисбалансу сил та інтересів			Більше 0,75	Безпосередня інформаційна загроза

Висновки

Таким чином, одержано достатньо чіткий критерій визначення характеру інформаційної небезпеки, який виходить із чисельних значень індексу інформаційної небезпеки. За допомогою цього критерію можна також уточнювати і рівні стабільності у суспільстві у випадках, коли сукупність значень величин $К_{про}$ і G суттєво відрізняються від прийнятих та отриманих у [3] орієнтовних інтервалів. Крім того розрахунок індексу інформаційної небезпеки та визначення відповідного характеру інформаційної небезпеки дає змогу шляхом рішення оберненої задачі зробити за допомогою табл. 1 впевнений висновок щодо рівня стабільності у суспільстві.

Переходячи до розгляду питання про критерій оцінки рівня інформаційної небезпеки, зауважимо, що реакція організації на інформаційну небезпеку різних рівнів відрізняється, перш за все, оперативністю і масштабами заходів, що здійснюються з метою досягнення бажаного рівня безпеки.

Отже, критерій оцінки рівня інформаційної небезпеки має опиратися, головним чином, на характер інформаційної небезпеки з обов'язковим урахуванням її масштабу. Обидва показники мають кількісний вимір, однак безпосереднє зведення їх до одного узагальненого показника не має підстав через принципову різницю між явищами, що ними характеризуються. Тому найбільш раціональним шляхом є логічний аналіз.

Таким чином, одержано достатньо чіткий критерій визначення характеру інформаційної небезпеки, який виходить із чисельних значень індексу інформаційної небезпеки. За допомогою цього критерію можна також уточнювати і рівні стабільності у суспільстві у випадках, коли сукупність значень величин $К_{про}$ і G суттєво відрізняються від прийнятих та отриманих у [3] орієнтовних інтервалів. Крім того розрахунок індексу інформаційної небезпеки та визначення відповідного характеру інформаційної небезпеки дає змогу шляхом рішення оберненої задачі зробити за допомогою табл. 1 впевнений висновок щодо рівня стабільності у суспільстві.

Переходячи до розгляду питання про критерій оцінки рівня інформаційної небезпеки, зауважимо, що реакція організації на інформаційну небезпеку різних рівнів відрізняється, перш за все, оперативністю і масштабами заходів, що здійснюються з метою досягнення бажаного рівня безпеки.

Отже, критерій оцінки рівня інформаційної небезпеки має опиратися, головним чином, на характер інформаційної небезпеки з обов'язковим урахуванням її масштабу. Обидва показники мають кількісний вимір, однак безпосереднє зведення їх до одного узагальненого показника не має підстав через принципову різницю між явищами, що ними характеризуються. Тому найбільш раціональним шляхом є логічний аналіз.

Таким чином, кожному рівню інформаційної небезпеки відповідає свій рівень інформаційної безпеки. Отже, критерієм оцінки рівня інформаційної безпеки є рівень інформаційної небезпеки.

Список літератури

1. Ануреев И.П. Применение математических методов в военном деле / И.П. Ануреев, А.Д. Татарченко. – М.: Воениздат, 1967. – 242с.

2. Чередниченко В.С. Обґрунтування пріоритетних заходів, щодо підвищення рівня інформаційної безпеки / В.С. Чередниченко // Захист інформації, Спец.випуск, 2008. – С. 13-15.

3. Хорошко В.О. Методичний підхід щодо оцінки рівня безпеки інформації / В.О. Хорошко, В.С. Чередниченко // Збірник наукових праць Військового інституту RYE ім. Т. Шевченка. – К., 2008. – Вип. 14. – С. 176-181.

4. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є.Шелест. – К.:ДУІКТ, 2008. – 186 с.

5. Козелецкий Ю.А. Психологическая теорія решений / Ю.А. Козелецкий. М.: Прогресс, 1979. –504 с.

Надійшла до редколегії 17.01.2013

Рецензент: д-р техн. наук, проф. О.О. Морозов, Академія внутрішніх військ МВС України, Харків.

МЕТОДИКА КОЛИЧЕСТВЕННО-КАЧЕСТВЕННОГО АНАЛИЗА И ОПРЕДЕЛЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Пузыренко, А.Ю. Иохов, А.М. Горбов, И.В. Кузьминич

В статье получен достаточно четкий критерий определения характера информационной опасности, который выходит из численных значений индекса информационной опасности. С помощью этого критерия стало возможно уточнять и ровная стабильность в обществе в случаях, когда совокупность значений величин коэффициенту проникновения и соотношения сторон существенно отличаются от известных.

Ключевые слова: *индекс информационной безопасности, уровень стабильности в обществе, коэффициент проникновения, вероятность предотвращения.*

METHOD OF QUANTITATIVE-HIGH-QUALITY ANALYSIS AND DETERMINATION OF INFORMATIVE STRENGTH SECURITY

O.G. Puzyrenko, O.Y. Iohov, A.M. Gorbov, I.V. Kuzminich

The clear enough criterion of determination of character of informative danger, which goes out from the numeral values of index of informative danger, is got In the article. By this criterion began possibly to specify even stability in society in the cases when aggregate of values of sizes it is substantially differed the coefficient of penetration and correlation of sides from known.

Keywords: index *of informative safety, level of stability in society, coefficient of penetration, probability of prevention.*