УДК 004.056.3

С.Ж. Піскун,
В.О. Хорошко, доктор технічних наук, професор
Ю.Є. Хохлачова

ОЦІНКА БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СФЕРИ

У статті викладено припущення про те, що рівень небезпеки інформації водночас характеризує й рівень безпеки інформації. Розглянуто поняття небезпеки та безпеки інформації, а також відмінності між ними й їх спільні сторони, взаємозалежність і її важливі риси. Розглянуто питання методичних основ оцінювання рівня безпеки інформації. Наведено схему подій, пов'язаних із забезпеченням безпеки інформації.

Ключові слова: *захист інформації, безпека інформації, небезпека інформації, оцінка рівня безпеки інформації, індекс безпеки інформації.*

В статье изложено предположение о том, что уровень опасности информации одновременно характеризует также уровень безопасности информации. Рассмотрены понятия опасности и безопасности информации, а также различия между ними и общие стороны, взаимозависимость и ее важные черты. Изучены вопросы методических основ оценки уровня безопасности информации. Приведена схема событий, связанных с обеспечением безопасности информации.

Ключевые слова: *защита информации, безопасность информации, опасность информации, оценка уровня безопасности информации, индекс безопасности информации.*

In this paper we prove the assumption that the level of hazard information simultaneously characterizes safety information as well. The concepts of risk and safety information as well the differences between them and their important features are considered. The issues of methodological foundations of an evaluation of information security are studied. A pattern of the events, associated with security information, is suggested.

Keywords: *information security, information policy, risk information, assessment of information security, information security index.*

Поняттю небезпеки інформації як наукової категорії і соціально-політичного явища протиставляється безпека інформації як рівень захищеності прав і свобод громадян, забезпечення розвитку суспільства та суверенітету держави. Із цього можна зробити висновок, що поняття безпеки інформації тісно пов'язане з поняттям національної безпеки.

У Законі України "Про основи національної безпеки України" вперше сформульовані й окреслені принципи національної безпеки. Пріоритетними завданнями української національної безпеки відповідно до нього визначено : створення внутрішніх, регіональних, світових умов мирного існування; добробут українського народу; демократичний розвиток суспільства; передбачення і відвернення інформаційних війн; протидія загрозам інформації.

При спільному розгляді понять небезпеки та безпеки інформації постає низка питань: яке з цих двох явищ є первинним, якими є їх взаємний зв'язок і взаємний вплив, якими можуть бути критерії їх оцінки?

Імовірно, що первинним є поняття небезпеки інформації. Саме на противагу небезпеці інформації визначаються шляхи, способи та засоби забезпечення безпеки інформації.

Незважаючи на смислову протилежність понять небезпеки інформації і безпеки інформації, між ними можна знайти багато спільного.

По-перше, обидва явища цілеспрямовано виникають в однакових сферах людської діяльності – політиці, економіці, ідеології, військовому будівництві тощо.

По-друге, небезпека інформації і безпека інформації створюються однаковими суб'єктами – державою, соціальними верствами, організаціями, підприємствами, людьми.

По-третє, і небезпека, і безпека інформації можуть створюватися однаковими засобами.

Що стосується відмінностей між небезпекою інформації і безпекою інформації, то вони знаходяться в різних площинах.

У першу чергу, це відмінність предметів небезпеки інформації та безпеки інформації стосовно об'єктів діяльності: предмет небезпеки інформації – оволодіння, опанування, загарбання, отримання, у той час як предмет безпеки інформації – захист, збереження, забезпечення умов для безперешкодного існування, зберігання, використання.

Інша принципова різниця між небезпекою інформації і безпекою інформації полягає в їх взаємовідносинах із об'єктами діяльності. Небезпека інформації є для своїх об'єктів зовнішнім, ворожим фактором. Безпека інформації об'єднана зі своїми об'єктами спільністю державної, комерційної, особистої таємниці, а також єдністю цілей та інтересів, особливо в екстремальних ситуаціях. У просторовому уявленні об'єкти безпеки інформації неначе оточені захисною оболонкою, а небезпека інформації спрямована на несанкціоноване її отримання та руйнування як самого цього захисту, так і самої інформації (об'єкта).

Нарешті, небезпека інформації і безпека інформації різняться ще й тими арсеналами засобів, за допомогою яких ці явища створюються у сфері життєвого циклу інформації. Якщо для небезпеки інформації це, насамперед, засоби впливу та впливу на неї, то безпека інформації, яка теж спирається на активну протидію, має досягатися, перш за все, шляхами запобігання несанкціонованим діям впливів на інформацію.

Взаємозалежність небезпеки інформації і безпеки інформації є беззаперечною. Вона має кілька важливих рис, які значною мірою впливають на ситуацію навколо інформації.

По-перше, це стримуючий вплив безпеки інформації на небезпеку інформації. Заходи, що вживаються державними та приватними організаціями за напрямом забезпечення інформаційної безпеки, зменшують імовірність несанкціонованих дій та впливів. Той самий стримуючий вплив безпеки інформації, якщо він здійснюється переважно одним типом захисту, часто виявляється тимчасовим, якщо не усунені первинні причини конфліктної ситуації або не застосовано комплексну систему захисту.

По-друге, має місце стимулюючий вплив небезпеки інформації на безпеку інформації. Будь-яке зростання небезпеки інформації викликає в суспільстві

іншу реакцію, яка, звичайно, виражається у зростанні зусиль та зміцненні комплексної системи захисту інформації.

При цьому особливої актуальності набуває питання методичних основ оцінки рівня безпеки інформації. Логічні методи аналізу проблем безпеки інформації є досить ефективними, однак вони не дають змоги встановити чіткі функціональні зв'язки між дією окремих чинників та їх сукупним результатом. Тому загальною потребою є розробка методики кількісно-якісного аналізу та об'єктивного визначення рівня безпеки інформації.

Під час розгляду поняття небезпеки інформації слід дійти висновку про те, що небезпеку інформації можна оцінювати за допомогою інтегрального показника (рівня небезпеки інформації), пов'язаного у певний спосіб зі ступенем застосування ситуації та очікуваним масштабом потенційного впливу. Переходячи до питання оцінки рівня безпеки інформації, необхідно, перш за все, з'ясувати сутність цієї оцінки.

По-перше, слід з'ясувати, чи можна говорити про безпеку інформації за умови відсутності небезпеки інформації. Очевидно, можна, оскільки безпека інформації, власне, і полягає у відсутності небезпеки інформації. Таким чином, повна відсутність небезпеки інформації означає повну безпеку інформації.

По-друге, слід з'ясувати, чи можна говорити про безпеку інформації за умови наявності небезпеки інформації. Очевидно, можна, однак вже з певним застереженням: чим вищий рівень небезпеки інформації, тим, мабуть, менше підстав стверджувати про безпеку інформації.

Складається думка про те, що сама по собі небезпека інформації достатньою мірою характеризує безпеку інформації. Цей парадоксальний, на перший погляд, висновок може бути досить переконливо доведений.

Як відзначалося раніше[1], безпека інформації досягається двома основними шляхами:

– відвернення впливу, пов'язаного з застосуванням пасивних та активних дій щодо можливого зловмисника, тобто використання для впливу на нього економічних, ідеологічних та інших важелів з метою відвернення спроб вирішення конфліктної ситуації;

– протидія впливу, тобто стримуванням (або відбиттям) впливу, шляхом застосування певних методів та засобів.

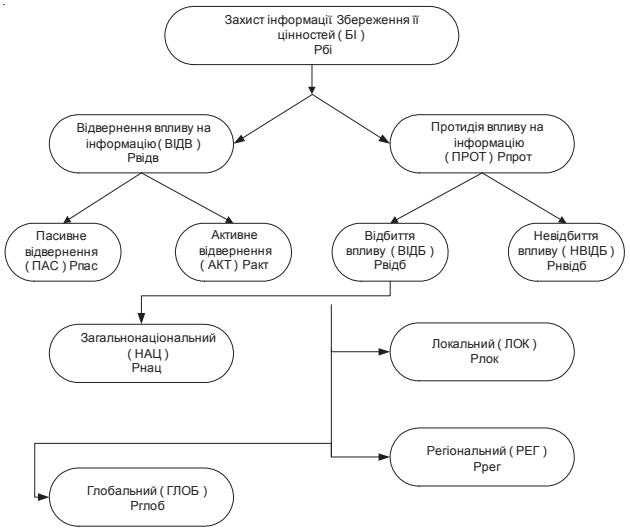

Рис. 1. Схема подій, пов'язаних із забезпеченням безпеки інформації

У центрі наших міркувань – потенційний вплив на інформацію як деяка подія, що може відбутися або не відбутися, залежно від ступеня зацікавленості в ній зловмисника – потенційного зловмисника, та від ефективності системи забезпечення безпеки інформації – об'єкта потенційного впливу. Якщо вплив на інформацію вдалося відвернути, то безпеку інформації забезпечено. Якщо атака все ж таки розпочалася, то можливість забезпечення безпеки інформації, ще зберігається через можливість успішної протидії впливу. При цьому подія може, залежно від рівня впливу, набути локального, регіонального, загальнонаціонального або глобального масштабу. Ототожнюючи небезпеку інформації з потенційним впливом та його наслідками, а безпеку інформації – з успішним захистом (у будь-який спосіб) інформації та збереження її цінності, можна побудувати відповідну схему подій, пов'язану з реалізацією небезпеки інформації та із забезпеченням безпеки інформації (рис. 1). Головними є такі пари протилежних подій:

– відвернення впливу та протидія йому;

– пасивне відвернення та активне відвернення впливу;

– відбиття впливу та його успіх.

Для аналізу взаємозв'язку цих подій може бути використано математичний апарат теорії ймовірностей. Проте звернення до теорії ймовірностей у цьому випадку потребує певного обгрунтування.

Справа в тому, що теорія ймовірностей оперує, як правило, подіями та явищами, які мають таку властивість як статистична стійкість. Історія людства дає нам тисячі прикладів конфліктів, але умови їх виникнення, розвитку і завершення є настільки різноманітними, що виділити стійкі статистичні ознаки дуже складно. Проте існує чимало аргументів на користь того, що імовірнісний підхід має право на застосування і в цій сфері.

Теорія ймовірностей має багато способів, що дають змогу визначати імовірності подій побічно, через імовірності інших подій, пов'язаних із першими [2].

Значну допомогу у вирішенні зазначеної проблеми може дати використання широко відомого принципу невизначеності Лапласа, суть якого полягає в тому, що за наявності кількох гіпотез, жодній з яких не можна віддати перевагу, слід вважати імовірності настання відповідних подій однаковими або рівноймовірними. Оскільки в нашому випадку розглядаються пари протилежних подій, то вихідною точкою може служити та аксіома, що для таких подій сума ймовірностей їх настання дорівнює одиниці.

Такими є принципові основи для застосування теорії ймовірностей в інтересах дослідження механізмів виникнення та припинення конфліктів і впливів в інформаційному колі [3].

Повертаючись до рис. 1, зауважимо, що тут подія, яка полягає у забезпеченні безпеки інформації, позначена через *БІ*, а її імовірність – через $P_{БІ}$. Ця подія може відбутися одночасно з однією із двох інших несумісних подій: з відверненням впливу (*ВІДВ*) з імовірністю $P_{відв}$ або з протидії впливу (*ПРОТ*) з імовірністю $P_{прот}$. При цьому, оскільки події (*ВІДВ*) та (*ПРОТ*) утворюють повну групу, то

$$P_{прот} = 1 - P_{відв} \qquad (1)$$

Розглядаючи настання подій *ВІДВ* і *ПРОТ* за умов конкретного рівня небезпеки інформації як лише дві можливі гіпотези, у зв'язку з якими з імовірністю

$P_{БІ}$ може стати подія *БІ*, відповідно до формули повної імовірності [2] можна записати:

$$P_{БІ} = P_{відв} * P_{(БІ / ВІДВ)} + P_{прот} * P_{(БІ / ПРОТ)} \quad (2),$$

або з урахуванням (1)

$$P_{БІ} = P_{віді} * P_{(БІ / ВІДВ)} + (1 - P_{відв}) * P_{(БІ / ПРОТ)} \quad (3),$$

де

$P_{БІ / ПРОТ}$ – умовна імовірність настання події *БІ* у разі настання події *ПРОТ*;

$P_{БІ / ВІДВ}$ – умовна імовірність настання події *БІ* у разі настання події *ВІДВ*.

Зауважимо, що настання події *ВІДВ* означає, що вплив відвернено, небезпека інформації нейтралізована. У такому випадку подія *БІ* є достовірною, тобто

$$P_{(БІ / ВІДВ)} = 1 \quad (4).$$

Якщо настала подія *ПРОТ*, то імовірність події *БІ* визначається, по суті, імовірністю успішного відбиття впливу на інформацію $P_{відв}$, тобто

$$P_{(БІ / ВІДВ)} = P_{відв} \quad (5).$$

Тоді, з урахуванням (4) і (5),

$$P_{БІ} = P_{відв} + (1 - P_{відв}) * P_{відв} \quad (6).$$

При цьому важливо визначитися з фізичним змістом величини $P_{відв}$. Якщо позначити максимальний прогнозований збиток для організації внаслідок зовнішнього впливу на інформацію як $G_{\max}$, то будемо вважати, що за певної імовірності відбиття впливу $P_{відв}$ збиток складе величину $G_{\max}(1 - P_{відв})$, а при $P_{відв} = 1$ (гіпотетичний випадок) величина збитку буде близькою до нуля.

Подальший розгляд взаємозв'язку подій може бути здійснено за такою схемою. Імовірність відвернення впливу шляхом пасивних дій (*ПАС*) або активного стримування впливу (*АКТ*) визначається таким рівнянням:

$$P_{відв} = P_{пас} + (1 - P_{пас}) * P_{акт} \quad (7).$$

Зауважимо, що імовірність стримування або відвернення впливу можна з певною мірою припущення порівняти з імовірністю її успішного відбиття, оскільки потенційний нападник, приймаючи рішення про несанкціоноване отримання інформації, рахується, передовсім, з можливостями сторони, яка захищає інформацію. З урахуванням цього можна записати рівняння (7) у вигляді

$$P_{відв} = P_{пас} + (1 - P_{пас}) * P_{відб} \quad (8).$$

Що стосується відбиття впливу на інформацію, яку захищаємо, то вона може відбуватися за умов її локального, регіонального, загальнонаціонального або глобального характеру, причому імовірності відповідних гіпотез утворюють повну групу

$$P_{лок} + P_{рег} + P_{нац} + P_{глоб} = 1 \quad (9).$$

Тоді:

$$P_{відб} = P_{лок} * P_{відб(лок)} + P_{рег} * P_{відб(рег)} + P_{нац} * P_{відб(нац)} + P_{глоб} * P_{відб(глоб)} \quad (10),$$

де

$P_{відб(лок)}, P_{відб(рег)}, P_{відб(нац)}, P_{відб(глоб)}$ – імовірності відбиття впливу відповідного характеру.

З урахуванням (8) і (10) рівняння (6) являє собою математичну модель, яка відображає ступінь загострення конфліктної ситуації та можливість щодо її вирішення шляхом відвернення або протидії впливу.

Проведені дослідження дають змогу визначити показники, які дозволяють зробити кількісну оцінку рівня безпеки інформації:

Як основний кількісний показник рівня безпеки інформації може бути прийнята імовірність успішного захисту інформації, збереження її цілісності за умов прогнозованої небезпеки інформації. Цей показник можна назвати індексом безпеки інформації, кількісне значення якого дає змогу робити певні висновки щодо рівня безпеки інформації.

Методика розрахунку індексу безпеки інформації має опиратися на результати оцінки небезпеки інформації, оскільки схеми подій, пов'язаних із забезпеченням безпеки інформації та з реалізацією небезпеки інформації, є аналогічними і характеризуються ймовірностями однакових подій. Крім того, основні вихідні данні для обчислення індексу безпеки інформації можуть бути віднесені до показників, що характеризують небезпеку інформації, а їх кількісні значення можуть визначатися під час оцінки останньої.

Отже, наведене вище припущення про те, що рівень небезпеки інформації одночасно характеризує й рівень безпеки інформації, можна вважати доведеним.

З огляду на взаємозалежність небезпеки інформації і безпеки інформації як основний кількісний показник небезпеки інформації може бути прийнята імовірність заподіяння суттєвої шкоди цілісності та цінності інформації, внаслідок впливу ззовні. Цей показник доцільно назвати індексом небезпеки інформації, який у співставленні з масштабом небезпеки інформації дає змогу за наявності певного критерію визначати рівень небезпеки інформації.

Індекси небезпеки інформації і безпеки інформації є ймовірностями протилеж-них подій, які, за визначенням, є несумісними і утворюють повну групу,

тобто

$$P_{НБІ} = 1 - P_{БІ} \quad (11)$$

Рівняння (11) дає змогу стверджувати про можливість застосувань єдиного методичного підходу до оцінки індексів небезпеки інформації і безпеки інформації.

Сама по собі кількісна оцінка індексу безпеки інформації, зважаючи на неминучі похибки, внаслідок неточності вихідних даних, не може мати переважного

значення. Більш важливим є інше: математичне моделювання індексу безпеки інформації має не тільки практичну, але й прогностичну цінність. Оперуючи значеннями змінних величин, що входять до математичних залежностей для обчислення індексу безпеки інформації, можна оцінювати ефективність впровадження тих чи інших заходів, спрямованих на його зниження. Тому функціональна залежність між індексом безпеки інформації і значеннями часткових показників обставин навколо інформації може бути інструментом поглибленого дослідження проблеми безпеки інформаційної сфери.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Хорошко В.О.* Методичний підхід щодо оцінки рівня безпеки інформації / В.О. Хорошко, В.С. Чередниченко // Зб. наук. праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – № 14. – С. 176–181.

2. *Феллер В.* Введение в теорию вероятностей и ее приложения : В 2-х т. / В. Феллер. – М. : Мир, 1967.

3. *Дружинин В.В.* Введение в теорию конфликта / В.В. Дружинин, Д.С. Конторов, М.Д. Конторов. – М. : Радио и связь, 1989. – 298 с.

Отримано 11.03.2013