УДК 004. 056:004.932

А.Г. Габович, А.Ю. Горобець, В.О. Хорошко
Державний університет інформаційно-комунікаційних технологій,
кафедра систем захисту інформації

МЕТОДИКА ОЦІНКИ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Розглянуто поняття безпеки і небезпеки інформації, яке з двох понять є первинним, якими є їхній взаємний зв'язок і взаємний вплив. Також наведена розроблена методика оцінки рівня безпеки інформації.

In article are considered notions of information security and information danger, which of two notions is initial which are their intercoupling and mutual influence. Is also brought designed methods of the estimation level to information security.

Вступ. Небезпеці інформації як соціально-політичному явищу і науковій категорії протиставляється безпека інформації як стан захищеності прав і свобод громадян, базових інтересів та цінностей суспільства і суверенності держави. Тому поняття безпеки інформації тісно пов'язано з поняттям національної безпеки.

Відомо, що основні ідеї сучасного розуміння національної безпеки вперше сформульовані у Законі України "Про основи національної безпеки України". Для України головна сфера національної безпеки – це створення внутрішніх, регіональних, світових умов мирного існування, добробуту українського народу, сталого демократичного розвитку суспільства. Це передбачає, зокрема, недопущення інформаційних війн, активну протидію загрозам інформації, виключення інформаційної ізоляції.

Фундаментом національної безпеки України є економічна безпека. Саме за умов стійкої економічної безпеки можливе вирішення усіх інших завдань забезпечення національної безпеки, тобто створення необхідних умов для стабільного розвитку економічних, соціально-політичних, духовно-інтелектуальних, екологічних та інших засад суспільства. З іншого боку, справжня інформаційна безпека існує тільки за умови надійного захисту національних інтересів України від будь-якого силового чи інформаційного тиску. Тому серед головних передумов національної безпеки України її інформаційну безпеку треба розглядати поряд з економічною та військовою безпеками, а за певних умов інформаційна безпека може набувати пріоритетного значення.

Істотним є співвідношення понять "безпека інформації" і "захист". Призначенням захисту є відвернення і відбиття атаки на інформацію або несанкціонованого її отримання. Безпека інформації порівняно з захистом явище значно складніше, багатоаспектніше й комплексніше. Безпеки інформації досягають не тільки за рахунок організації захисту інформації, вона передбачає різноманітні заходи також і в політичній, економічній та інших сферах суспільного життя.

Аналіз сучасного етапу проблеми рівня безпеки інформації. При спільному розгляді понять небезпеки інформації та безпеки інформації виникає низка питань: яке з цих двох явищ є первинним, якими є їхній взаємний зв'язок і взаємний вплив, якими можуть бути критерії їхні оцінки?

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

Проте, 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, економіки, ідеології, військовому будівництві тощо.

По-друге, небезпека інформації і безпека інформації створюються однаковими суб'єктами – державною, 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 лежать у різних площинах.

Передовсім, це відмінність предметів небезпеки інформації та безпеки інформації стосовно об'єктів діяння: предмет небезпеки інформації – оволодіння, опанування, загарблення, отримання, тоді як предмет безпеки інформації – захист, збереження, забезпечення умов для безперешкодного існування, зберігання, використання.

Інша принципова відмінність між небезпекою інформації і безпекою інформації у їхніх взаємовідносинах з об'єктами діяння. Небезпека інформації є для своїх об'єктів зовнішним, ворожим чинником. Безпека інформації об'єднана зі своїми об'єктами спільністю державної, комерційної, особистої єдністю цілей та інтересів, особливо в екстремальних ситуаціях. У просторовому уявленні об'єкти безпеки інформації наче 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 відрізняються ще й тими арсеналами засобів, за допомогою яких ці явища створюються у сфері життєвого циклу інформації. Якщо для небезпеки інформації це, насамперед, засоби атаки та впливу на неї, то безпека інформації, яка теж спирається на активні протидії, має досягатися, насамперед, запобіганням несанкціонованим діям та атакам 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 вживають державні та приватні організації в напрямі забезпечення інформаційної безпеки, зменшують імовірність несанкціонованих дій та атак. Водночас стримуючий вплив безпеки інформації, якщо він здійснюється переважно одним типом захисту, часто виявляється тимчасовим, якщо не усунути первинні причини конфліктної ситуації або не застосувати комплексну систему захисту.

По-друге, відзначається стимулюючий вплив небезпеки інформації на безпеку інформації. Будь-яке зростання небезпеки інформації викликає у суспільстві ту або іншу реакцію, яка звичайно виражається у зростанні зусиль та зміцненні комплексної системи захисту інформації.

Дуже актуальним є питання методичних основ оцінки рівня безпеки інформації. Логічні методи аналізу проблем безпеки інформації є доволі ефективними, однак вони не дають змоги встановити чіткі функціональні зв'язки між дією окремих чинників та їхнім сукупним результатом. Тому нагальною потребою є розроблення методики кількісно-якісного аналізу та об'єктивного визначення рівня безпеки інформації.

Методика оцінки рівня безпеки. Розглядаючи поняття небезпеки інформації, можливо 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 потенційної атаки. Переходячи до питання оцінки рівня безпеки інформації, необхідно передовсім з'ясувати сутність цієї оцінки.

Сформулюємо для себе декілька запитань, на які і дамо відповіді.

По-перше, чи можна говорити про безпеку інформації за умови відсутності небезпеки інформації? Очевидно, можна, оскільки безпека інформації, власне, і полягає у відсутності небезпеки інформації. Отже, повна відсутність небезпеки інформації означає повну безпеку інформації.

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

Виникає думка, що сама по собі небезпека інформації достатньою мірою характеризує безпеку інформації. Цей парадоксальний, на перший погляд, висновок може бути, проте, досить твердо доведений.

Як відзначалось в [1], безпека інформації досягається двома основними способами:

1 відветанням атаки, пов'язаним із застосуванням пасивних та активних дій щодо можливого зловмисника, тобто використання для впливу на нього економічних, ідеологічних та інших важелів, щоб запобігати спробам вирішення конфліктної ситуації;

2 протидією атаці, тобто стримуванням (або відбиттям) атаки застосуванням певних методів та засобів.

Стримуючий вплив на потенційного зловмисника має сам факт наявності у об'єкта атаки серйозної системи захисту та інших заходів відвернення атаки на інформацію.

Схема подій, по'язаних із забезпеченням безпеки інформації

У центрі наших міркувань потенційна атака на інформацію як деяка подія, що може відбутися або не відбутися залежно від ступеня зацікавленості в ній порушника – потенційного зловмисника та від ефективності системи забезпечення безпеки інформації – об'єкта потенційної атаки. Якщо атаку на інформацію вдалося відвернути, то безпеку інформації забезпечено. Якщо атака все ж таки розпочалася, то можливість забезпечення безпеки інформації, проте, ще зберігається через можливість успішної протидії атаці. Подія, яка може, залежно від рівня атаки, набути локального, регіонального, загальнонаціонального або глобального масштабу.

Ототожнюючи небезпеку інформації з потенційною атакою та її наслідками, а безпеку інформації – з успішним захистом (у будь-який спосіб) інформації та збереженням її цінності, можна побудувати відповідну схему подій, пов'язану з реалізацією небезпеки інформації та із забезпеченням безпеки інформації (див. рисунок). Головними є такі пари протилежних подій:

1 відвернення атаки та протидія їй;

2 пасивне та активне відвернення атаки;

3 відбиття атаки та її успіх.

Для аналізу взаємозв'язку цих подій може бути використано математичний апарат теорії імовірностей. Проте звернення до теорії імовірностей у такому разі потребує певного обгрунтування.

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

Теорія імовірностей має багато способів, що дають змогу визначати імовірності подій непрямо, через імовірності інших подій, пов'язаних з першими [2].

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

Такими є принципові основи для застосування теорії імовірностей в інтересах дослідження механізмів виникнення та припинення конфліктів і атак в інформаційному колі.

До речі, імовірнісний підхід під час аналізу конфліктних ситуацій застосовують і зарубіжні

дослідники [3].

Повертаючись до рисунка, 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 атаки (ВІДВ) з імовірністю $P_{відв}$ або з протидії атаки (ПРОТ) з імовірністю $P_{прот.}$ Оскільки події ВІДВ та ПРОТ утворюють повну групу несумісних подій, то

$$P_{прот} = 1–P_{відв}. \quad (1)$$

Розглянемо настання подій ВІДВ і ПРОТ за умови конкретного рівня небезпеки інформації як лише дві можливі гіпотези, у зв'язку з якими з імовірністю $P_{бі}$ може стати подія БІ, що відповідно до формули повної імовірності [2] можна записати

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

або з урахуванням (1)

$$P_{бі} = P_{відв} \cdot P(БІ/ВІДВ) + (1–P_{відв}) \cdot P(БІ/ПРОТ), \quad (3)$$

де P(БІ/ВІДВ) – умовна імовірність настання події БІ у разі настання події ВІДВ; P(БІ/ПРОТ) – умовна імовірність настання події БІ у разі настання події ПРОТ.

Зауважимо, що настання події ВІДВ означає, що атака відвернена, небезпека інформації нейтралізована. У такому разі подія БІ є достовірною, тобто

$$P(БІ/ВІДВ) =1. \quad (4)$$

Якщо настала подія ПРОТ, то імовірність події БІ визначається, власне кажучи, імовірністю успішного відбиття атаки на інформацію ($P_{відв}$), тобто

$$P(БІ/ВІДВ) = P_{відв}. \quad (5)$$

Тоді, з урахуванням (4) і (5)

$$P_{бі} = P_{відв} + (1 – P_{відв}) \cdot P_{відв}. \quad (6)$$

Важливо визначитися з фізичним поняттям величини $P_{відв}$. Якщо позначити максимальний прогнозований збиток для організації внаслідок зовнішньої атаки на інформацію як G_{max}, то будемо вважати, що за певної імовірності відбиття атаки $P_{відв}$ збиток становитиме $G_{max}(1 – P_{відв})$, а при $P_{відв} \equiv 1$ (гіпотетичний випадок) розмір збитків буде близьким до нуля.

Подальший розгляд взаємозв'язку подій, наведених на рисунку, може бути здійснено за аналогічною схемою. Імовірність відвернення атаки за допомогою пасивних дій (ПАС) або активного стримування атаки (АКТ) визначається таким рівнянням:

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

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

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

Що стосується відбиття атаки на інформацію, що захищається, 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

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

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

З урахуванням (8) і (10) рівняння (6) становить собою математичну модель, яка відображає ступінь загострення конфліктної ситуації та можливість щодо її вирішення через відвернення або протидію атаці.

Дослідження дають змогу зробити такі висновки:

1. 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.

2. Методика розрахунку індексу безпеки інформації має спиратися на результати оцінки небезпеки інформації, оскільки схеми подій, пов'язаних із забезпеченням безпеки інформації та з реалізацією небезпеки інформації, аналогічні і характеризуються імовірностями однакових подій. Крім того, основні вихідні дані для обчислення індексу безпеки інформації можуть бути зараховані до показників, що характеризують небезпеку інформації, а їхні кількісні значення можуть визначатися під час оцінки останньої.

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

3. Зважаючи на взаємозалежність небезпеки інформації і безпеки інформації, як основний кількісний показник небезпеки інформації може бути прийнята імовірність заподіяння істотної шкоди цілісності та цінності інформації внаслідок атаки ззовні. Цей показник доцільно назвати індексом небезпеки інформації, який порівняно з з масштабом небезпеки інформації дає змогу, за наявності певного критерію, визначати рівень небезпеки інформації.

4. Індекси небезпеки інформації і безпеки інформації є імовірностями протилежних 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 застосування єдиного методичного підходу до оцінки індексів небезпеки інформації і безпеки інформації.

5. Сама по собі кількісна оцінка індексу безпеки інформації, зважаючи на неминучі похибки внаслідок неточності вихідних даних, не може мати переважного значення. Важливішим 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 обстановки навколо інформації може бути інструментом поглибленого дослідження проблеми безпеки інформації.

1. Лузянин В.П. Методология исследования проблем безопасности и стабильности // Военная мысль. – 1993. – №3. – С. 34–39. 2. Вентцель Е.С. Теория вероятностей. – М., 1962. 3. Саати Т.Л. Математические модели конфликтных ситуаций. – М., 1997.

УДК 004.05 (07)

П.В. Мокренко
Національний університет "Львівська політехніка",
кафедра автоматики та телемеханіки

ПРО СИСТЕМНУ КОНЦЕПЦІЮ