- звуковий супровід – за допомогою авторського права;
- зображення, що виводяться програмою – за допомогою авторського права;
- назву – на підставі свідоцтва на знаки для товарів і послуг;
- логотип (торгівельну марку) – на підставі свідоцтва на знаки для товарів і послуг;
- дизайн інтерфейсу – за допомогою авторського права.

Саме така система правової охорони буде перешкоджати неправомірному використанню як самої комп'ютерної програми, так і тотожної їй, що написана іншою особою за тим самим алгоритмом та призводить до однакового технічного результату.

Ще одним рішенням цієї проблеми є застосування спеціального системного підходу, з використанням авторського, патентного, договірного права, законодавства про недобросовісну конкуренцію, про комерційну таємницю тощо, або створення спеціальної правової системи охорони комп'ютерної програми, що на сьогодні впроваджено у деяких країнах світу.

Наприкінці хотілось би висловити сподівання щодо розробки нових нормативно-правових актів та внесення необхідних змін та доповнень у чинне законодавство з метою зменшення в Україні рівня піратства на ринку програмного забезпечення, що дозволить швидко розвиватися національним розробникам комп'ютерних програм.

*Література: **1**. Про авторське право і суміжні права: Закон України // Відомості Верховної Ради України. - 2001. - 43. - с. 214. **2**. Бабаев В. Виды объектов интеллектуальной собственности в иновационной деятельности // Підприємство, господарство і право - 2003. - № 9. - с. 68 - 71. **3.**. Музика А., Азаров Д. Про поняття злочинів у сфері комп'ютерної інформації//Право України.- 2003. - № 4. - с. 86 - 89. **4.** Смирнова Н. Програмний продукт: твір, винахід, або унікальний кумулятивний об'єкт // Інтелектуальна власність - 2003. - № 5. - с. 9 - 12. **5**. Словарь иностранных слов и выражений/ Авт. И сост. Е. С. Зенович. - М.: ООО «Фирма «Издательство АСТ»,2000 – 784 с. **6.** Жуванов Д., Стогній Є. Яку форму правової охорони обрати для комп'ютерної програми // Інтелектуальна власність - 2003. - № 9. - с. 37 - 42. **7**. Тимофієнко Л., Ліннік Л. Правова охорона комп'ютерних технологій // Інтелектуальна власність - 2001. - № 4. - с. 12 - 17. **8.** Остапчук В. Останні зміни в режимі захисту прав інтелектуальної власності // Юридичний журнал - 2004. - № 1(19). - с. 60 - 65. **9**. Цивільний кодекс України (від 16 січня 2003 року) // Українська інвестиційна газета. - 2003. – 194 с. **10.**. Ладник В. Доцільність і можливість охорони комп'ютерних програм нормами патентного права / Інтелектуальна власність. - 2002. - № 9. - с.12 - 16. **11.**. Машуков В. М. Компьютерное право: практическое руководство.-Львов: Аверс, 1998. – 256 с. **12.** Вайшнурс А. Современность и перспективы правовой охраны баз данных России, США и Европейского союза.// Интеллектуальная собственность. Авторское право и смежные права. - 2003. - № 11. - с. 5 – 21. **13**. Трофименко А. Авторское право на результаты действия автоматических устройств.// Интеллектуальная собственность. Авторское право и смежные права. - 2004. - № 3. - с.12 - 18. **14**. Ханина К. Воздействия развития информационных технологий на формирование системы авторского права Европейского союза.// Интеллектуальная собственность. Авторское право и смежные права. - 2004. - № 3. - с. 27 - 36. **15**. Смирнов В. Еще раз об охране компьютерных программ // ИС. Промышленная собственность. - 2002. - № 2. - с. 42 - 47. **16**. Петренко С. Правовий захист комп'ютерних програм // Право України. - 2003. - № 3. - с. 108 - 111. **17.** Ващинець І. Проблеми удосконалення прав автора на розповсюдження у чинному законодавстві України// Інтелектуальна власність. - 2004. - № 1. – с. 11 - 17.*

УДК 681.5:621.391

МОДЕЛІ ЦІННОСТІ ІНФОРМАЦІЇ З ПОЗИЦІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО - ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Володимир Кононович, Микола Тардаскін, Тетяна Тардаскіна*

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком",
**Одеська національна академія зв'язку*

Анотація: **Аналізуються існуючі підходи до визначення цінності інформації. Запропоновано багатокритеріальну оцінку цінності з урахувнням властивостей інформації з позицій інформаційної безпеки. Приведені моделі цінності інформації в залежності від показників її обсягу, часу, конфіденційності, цілісності, доступності.**

Summary: **Substantial approaches are analyzed to determinate the information values. Multicriterial assessment of the information value depending on information property with viewpoint of information security is offering. Information model of value depending on scope, time, confidentiality, integrity end availability is considered.**
Ключові слова: **Інформаційна безпека, кількість інформації, ентропія, моделі цінності інформації, інформаційно-телекомунікаційні системи, загрози інформації, функція штафів.**

I Вступ

Однією з проблемних задач побудови комплексної системи захисту інформації (КСЗІ) є знаходження можливих втрат від реалізації специфікованої множини загроз. Визначення цінності інформації є критичними етапами у прийнятті рішень щодо управління обробкою інформації та її захисту. Оцінка цінності ресурсів, які захищаються, та аналіз загроз інформаційній безпеці проводиться з перших етапів життєвого циклу системи інформаційної безпеки: розробки технічного завдання чи технічних умов, технічного та робочого проектування. Більшість запропонованих стратегій [1…3] передбачає отримання величини або можливих збитків на кожному з класів порушень, або кількісних оцінок ризику чи залишкового ризику тощо. В [4] пропонується обчислення очікуваної величини втрат для кожної загрози у вигляді добутку $V \bullet p$: де V – грошова оцінка втрат від реалізації загрози, або відносна вартість інформаційного об'єкта; p – ймовірність реалізації загрози. Заходи протидії застосовують для зменшення залишкового ризику шляхом або зменшення ймовірності здійснення загрози, або зменшення ефекту впливу загрози. Кожен захід протидії, у свою чергу, характеризується ефективністю і вартістю. На основі оцінок загроз та оцінок ризику на наступних етапах побудови та експлуатації КСЗІ розробляються адекватні засоби і заходи захисту за принципом необхідної (розумної) достатності – витрати на інформаційну безпеку мають, принаймні, не перевищувати величини очікуваних втрат від можливої реалізації загроз.

В процесі оцінок виникає низка проблем. Деякі наслідки загроз (приміром – які спричиняють соціальні впливи) оцінюють за допомогою якісних шкал або оцінок типу: низький, середній, високий, недопустимо високий тощо ризик. Точна грошова оцінка загрози також може бути складною. В процесі визначення цінності інформації, крім можливих загроз, необхідно враховувати властивості самої інформації та дії зацікавлених сторін. Процес оцінки залишається надто суб'єктивним. Тому дослідження питань цінності інформації залишається актуальною задачею.

Метою роботи є аналіз теоретико-інформаційних методів оцінки цінності інформації з позицій інформаційної безпеки, в яких враховувались би інтегрально властивості конфіденційності, цілісності та доступності інформації. Методами прикладної теорії інформації та інформаційної теорії систем успішно вирішуються ряд задач в області складних комплексів, які включають в себе різнорідні системи, працюють в складних умовах і задовольняють сукупності різноманітних взаємно протилежних вимог, що є характерним, зокрема, для комплексних систем інформаційної безпеки інформаційно-телекомунікаційних систем.

II Теоретико-інформаційні підходи до оцінки кількості та цінності інформації

В різних областях науки і техніки вводяться свої визначення поняття інформації. У енциклопедичних словниках термін інформація (від лат. Informatio — роз'яснення, викладення) позначав відомості щодо змін, які передаються одними людьми іншим людям усним, письмовим чи якимось іншим способом, а також сам процес передавання чи одержання цих відомостей. В розширеному розумінні обмін відомостями здійснюється як між людиною і людиною, так і між людиною і автоматом, автоматом і автоматом тощо.

Більш точні визначення інформації у природничих та філософських науках виходять із факту, що інформація є фізичною величиною, що дозволяє сформулювати закони типу збереження [5], по аналогії із законами збереження енергії. Основна гіпотеза таких інформаційних теорій полягає в тому, що інформація завжди має матеріальний носій і представляє собою деякі властивості (стан) матерії. Відомості (інформація) створюються тоді, коли один об'єкт "передає" іншому об'єкту частину своїх властивостей. Інформація для одного об'єкта – це частина властивостей іншого об'єкта. За цих тверджень принциповий смисл закону збереження інформації полягає у тому, що коли якась властивість матеріального об'єкта (інформація) додається до системи, то із іншої системи вона зникає і навпаки. В тривіальному випадку приміром, втрата конфіденційності інформації власника означає її додавання до інформації зловмисника.

В точних науках поняття інформації (як і поняття алгоритму) вводиться аксіоматично. Міра кількості інформації вводиться строго, але склались різні підходи до визначення мір кількості та цінності інформації в залежності від призначення інформації. Міри кількості інформації відіграють важливу роль в процесах

обробки інформації, її зберігання, передавання, перетворення. В процесах застосування інформації для досягнення певної мети – управління, прийняття рішень, захисту – крім міри кількості мають значення міри цінності (корисності) інформації. При цьому, маючи дуальний характер, інформаційний ресурс виступає у двох ролях: одна його частина визначає структуру системи і забезпечує стабільність цієї структури, тобто стійкість відносно внутрішніх і зовнішніх впливів (тут на перший план виступають показники кількості, цілісності і доступності ресурсу); друга його частина, що може перетинатись з першою, виконує функції управління, визначає характер процесів, які протікають у системі (у цій частині більш важливі показники цінності, конфіденційності і спостереженості).

В роботах К. Шеннона, Р. В. Л. Хартлі, А. Н. Колмогорова, М. М. Бонгарда, А. А. Харкевича та ін. запропоновані кількісні міри інформації, перелічені в [6]. Із загальних позицій, чим більше різноманіття числа елементів *n* (будь-якої природи), тим більше інформації є у цьому різноманітті. В усіх мірах інформації використовуються або розподіл ймовірностей, якщо наявна множина елементів вибору, або безпосередньо міри складності (програми при алгоритмічному підході), або діапазон суб'єктивних інтересів, якщо розглядаються ергатичні чи антропологічні системи. Кількість інформації, що міститься у повідомленні і сигналі по К. Шеннону визначається їх ентропією, тобто зменшенням невизначеності при виборі:

$$H = -\sum_{i=1}^{n} P_i \log_2 P_i, \qquad (1)$$

де *n* – кількість можливих результатів вибору чи подій із скінченої множини подій; P_j – ймовірність *i* – го результату вибору чи події.

Ентропії притаманні такі властивості. Інформація є мірою, яка визначає порядок системи, а ентропія є обернена їй величина. Множину подій можна ототожнювати з множиною станів системи, в кожному з яких вона може опинитись з деякою ймовірністю. Ступінь невизначеності множини подій залежить не тільки від їх кількості, але і від ймовірностей, з якою вони виступають. Ентропію можна трактувати як число способів, яким може бути реалізований даний стан системи. Ентропія виражає ймовірність стану системи, зростання ентропії означає перехід системи від менш ймовірних станів до більш ймовірних.

Міра кількості інформації (1) введена так, що задовольняється властивість адитивності [7]: якщо групи випадкових подій ξ_1, ξ_2, незалежні, то повна (сумісна) ентропія розпадається на суму ентропій $H_{\xi1,\xi2} = H_{\xi1} + H_{\xi2}$. Теорему складання ентропій можна читати так: ентропія об'єднання незалежних систем дорівнює сумі індивідуальних ентропій систем. Крім того, ентропія має властивість ієрархічної адитивності. Так, ентропія у випадку нелінійного представлення інформації за допомогою гіпертекстової розмітки обчислюють як суму умовних ентропій

$$H_{\xi1\ldots\xi n} = H_{\xi1} + H_{\xi2/\xi1} + H_{\xi3/\xi1,\xi2} + \ldots + H_{\xi n/\xi1\ldots\xi n-1}.$$

На відміну від теоретико - ймовірнісного підходу Шеннона, ще раніше Хартлі на основі комбінаторних підходів пропонував визначати кількість інформації як логарифм різноманітності

$$H(X) = \log_2 n, \qquad (2)$$

де *n* – потужність скінченої множини *X*. Тут ентропія як міра різноманітності визначається лише числом подій (станів системи). Таку міру зручно застосовувати, коли станам системи неможливо приписати деякі ймовірності. Зауважимо, що для системи, яка має рівноймовірні стани, співвідношення (1) перетворюється у (2) та задає максимально можливу ентропію множини з *n* елементів.

Проста формалізація поняття кількості (корисної) інформації, яке застосовується в кількісній теорії інформації і висунуте в 1960 році А. А. Харкевичем, постулює, що цінність інформації (міра доцільності управління) визначається як логарифм приросту ймовірності досягнення даної мети в результаті використання даної інформації: $\log_2(p_1/p_0)$, де p_1 - ймовірність досягнення мети після виконання рішення, яке генероване на базі прийнятої інформації; p_0 - ймовірність досягнення мети до прийняття рішення.

Згідно з алгоритмічним підходом А. Н. Колмогорова [8] ентропія *H(x, y)* є мінімальна довжина записаної у вигляді послідовності нулів і одиниць "програми", яка дозволяє побудувати об'єкт *X,* маючи у своєму розпорядженні об'єкт *Y*, де *y* – відомості щодо ситуації чи об'єкта *x*. В термінах інформаційної безпеки можуть бути застосовані такі розуміння міри кількості інформації як логарифм числа спроб подолання (злому) системи захисту, або логарифм числа кроків алгоритму чи кількості команд програми, яка вирішує цю задачу. Алгоритмічний підхід удосконалено в інформаційній теорії систем [9], де прийнято визначати кількість інформації як

$$I = \sum_{i=1}^{n} I_{ki}, \qquad (3)$$

де n – число символів у самому короткому ланцюжку серед множини ланцюжків символів, кожна з яких є опис (модель) даної системи чи її частини; I_{ki} – кількість інформації, яка міститься у одному символі і визначається по Хартлі; $k = x, \varphi, \gamma, c,$ які визначаються у [9] як параметри алгебраїчної моделі системи.

Застосування апарату теорії інформації до проектування КСЗІ обумовлена тим, що у ряді випадків функціонування КСЗІ та управління інформаційною безпекою можна представити в концепціях вибору. Дійсно, сукупність можливих значень множини параметрів, які описують стан системи, можна представити сукупністю точок, що займають у багатомірному просторі параметрів гіпероб'єм V_0. Зміна параметрів системи буде виражатись переміщенням відображаючих точок всередині гіпероб'єму V. Від комплексу управління інформаційною безпекою вимагається здійснювати вибір гіпероб'єму V', який відповідає заданим параметрам КСЗІ, з усього гіпероб'єму V_0, у якому апріорі можуть знаходитись параметри системи. Вибір гіпероб'єму V' залежить як від функціонування КСЗІ, так і від зовнішніх відносно нього факторів: характеристик функціонування автоматизованої системи, реалізації зовнішніх та внутрішніх загроз, наявності антропогенних та техногенних впливів тощо. Мінімально необхідна кількість інформації I, яка має бути отримана і оброблена системою (або зловмисником) для вибору часткового гіпероб'єму V' із усього апріорного гіпероб'єму V_0, дорівнює ентропії зняття відповідної невизначеності H:

$$I = H = \log_2(V_0 / V') \text{ [біт]} \tag{4}$$

при рівноймовірному розподілу часткових гіпероб'ємів. Для виконання задач системою необхідно, щоб ця кількість інформації було оброблено за час, який не перевищує деяку величину T. Тоді мінімально необхідна швидкість отримання і оброблення інформації має становити

$$R = \frac{I}{T} = \frac{1}{T}\log_2\left(V_0 \Big/ V'\right). \tag{5}$$

Система працездатна, поки $R < C,$ тобто поки швидкість оброблення інформації R не досягає її інформаційної пропускної здатності C. Кількість оброблюваної інформації при застосуванні, приміром, засобів фільтрації від зовнішніх впливів на дану обчислювальну систему через засоби телекомунікаційної мережі, залежить від стійкості засобів фільтрації, характеристик системи управління доступом, коректності виконання процедур адміністрування, кількості можливих ідентифікаторів, кількості можливих варіантів паролів, надійності їх конфіденційного зберігання тощо.

III Поняття цінності інформації з позицій інформаційної безпеки

Ентропія як міра невизначеності не завжди дозволяє зв'язати цю міру з успішністю застосування інформації при вирішенні певних задач [10]. Ця міра не залежить від того, як буде використано повідомлення після його отримання, або який семантичний зміст буде впливати на прийняття рішень. Міра корисної інформації має відображати степінь корисності повідомлення для користувача. При цьому міра має залежати від того, яка задача вирішується, яка інформація була до приходу повідомлення і який семантичний зміст повідомлення (тобто, як трактується повідомлення користувачем).

Прагматична оцінка цінності інформації задається її класифікацією, при якій визначаються значущі властивості інформації та динаміка показників цих властивостей. По рівню важливості конкретну інформацію поділяють на чотири категорії [1]:

- життєво важлива – незамінима інформація, наявність якої необхідна для функціонування організації;
- важлива – інформація, яка може бути замінена чи відновлена з великими труднощами чи значними витратами;
- корисна – інформація та, яку важко відновити, але організація може ефективно функціонувати і без неї;
- несуттєва – інформація, яка більше не потрібна.

Категорії важливості певної інформації можуть з часом змінюватись. У різних підрозділах одна і та ж інформація може бути віднесена до різних категорій важливості. Цінність інформації може бути різною для різних груп осіб – власників, розпорядників, авторів, зловмисників.

З метою мати можливість проводити порівняльний аналіз різних систем, або порівнювати корисність вирішення різних задач, категорія цінності інформації має мати такі властивості:

- цінність інформації має бути зв'язана з кінцевим ефектом використання цієї інформації; чим кінцевий ефект більше, тим більше цінність інформації;
- цінність інформації зв'язується з функцією корисності, яка виражається у грошових одиницях; - показник цінності інформації зв'язується з критеріями оптимальності приймання та обробки інформації. В інформаційно-телекомунікаційних системах користувач і місце зберігання чи обробки інформації можуть

бути територіально рознесені;

- показник цінності інформації доцільно зв'язувати з властивостями інформації: конфіденційністю, цілісністю, доступністю; при цьому захищеність не є атрибутивною властивістю інформації; захищеність є зовнішньою властивістю, притаманною інформації, яка знаходиться в певній системі і змінюється при передаванні її в іншу систему; цінність технологічної інформації інформаційно-телекомунікаційних систем зв'язана безпосередньо з її конфіденційністю, а цінність публічної інформації підтримується її доступністю і цілісністю;
- мають відображатися суттєві сторони системи інформаційної безпеки (ризику, витрат тощо);
- має бути можливим вносити у формалізм теорії цінності інформації конкретний фізичний і технічний смисл, згідно з призначенням систем.

Ентропія завжди є невід'ємною (позитивною) величиною. Функція корисності може бути від'ємною (негативною), якщо керуюче рішення, прийняте на основі отриманої інформації, приносить збитки. Міра кількості корисної інформації вводиться так, що вона може бути як додатною так і від'ємною. Функція цінності інформації може приймати як додатні так і від'ємні значення (позитивна і негативна інформація). Негативна цінність означає, що для вирішення певної конкретної задачі ця інформація несуттєва або шкідлива. У багатьох випадках при вирішенні задачі інформація обробляється таким чином, щоб максимально скоротити несуттєву інформацію про об'єкт.

Існуючі підходи до проблеми цінності інформації можна згрупувати у такі напрями [6]: зв'язані з мінімізацією втрат (оборона інформаційних ресурсів); зв'язані з максимізацією виграшу (напад на інформаційні ресурси); враховуючі суб'єктивні фактори – цінність інформації для суб'єкта. Мінімізація витрат і максимізація виграшу не є двома випадками однієї задачі. Зловмисник може завдати значні збитки, витративши при цьому малі власні ресурси.

Теорія цінності інформації в [6] зв'язана з теорією статистичних рішень, де основою є поняття середніх втрат або ризику. Корисність інформації полягає в тому, що вона дозволяє зменшити втрати. Втрати зв'язуються з функцією штрафів. За більш вдалі рішення призначаються менші штрафи, ніж за менш вдалі. Мета полягає у мінімізації штрафів. Чим менше значення функції штрафів при отриманні деякої інформації, тим ця інформація цінніша. Роль функції штрафів можуть відігравати безпосередньо витрати, виражені у грошових одиницях. Кількісно цінність інформації визначається як та максимальна користь, яку дана кількість інформації може принести для зменшення середніх втрат. Конкретна форма виразів для мінімальних втрат розроблена в [6]. За міру цінності інформації T приймається різниця між значеннями функції втрат при відсутності інформації $R(0)$ та при її отриманні $R(I)$:

$$T(I) = R(0) - R(I), \tag{6}$$

При цьому величина втрат при отриманні інформації $R(I) = R_0(I) + R_o(I)$, де $R_0(I)$ – величина втрат, якщо інформаційний ресурс зберігає задані властивості конфіденційності, доступності, цілісності та спостережності; $R_o(I)$ – додаткові втрати при частковій чи повній втраті цих властивостей. При наявності системи інформаційної безпеки величина втрат стає рівною залишковим втратам $R(I) = R_з(I)$, зменшення яких викликане заходами і засобами захисту.

За функцію штрафів можна прийняти деяку міру труднощів вирішення задачі [10]. Такою моделлю є система, яка для вирішення задачі веде експериментальну роботу методом проб та помилок (пошуку вразливостей захищеної системи, підбору паролю, злому системи захисту тощо). У процесі спроб зловмисник має змогу здобувати деякі відомості щодо системи захисту і тим самим зменшувати невизначеність часткової задачі a для свого розв'язуючого алгоритму. Невизначеність задачі знаходиться як логарифм математичного очікування числа спроб, необхідних для вирішення задачі: $N = \log K(a)$.

У загальному випадку задачу можна сформулювати так. Нехай задана скінченна множина об'єктів, таких як вразливості автоматизованої системи, $M = \{m_i\}$, на якій задано розподіл ймовірностей $p(m_1), \ldots, p(m_i), \ldots, p(m_r)$. Приміром ймовірності можуть стосуватись блокування чи навпаки не заблокування відповідної вразливості засобами захисту. Ця множина розбита на n підмножин A_i (приміром, по типам вразливостей) таких, що $A_1 \cup A_2 \ldots \cup A_n = M$ та $A_i \cap A_j = \Phi$ при $i \neq j$. Вирішення задачі відносно деякого об'єкта m_i полягає у знаходженні такого i, що $m_i \in A_i$. Тепер, якщо задано розв'язуючий алгоритм (спосіб атаки на вразливість) відносно об'єкта m_i, то число застосувань алгоритму (спроб), яке приводить до успіху, є випадкова величина $K(m_i)$. Невизначеність задачі у відношенні до об'єкта m_i для даного розв'язуючого алгоритму є логарифм математичного очікування числа спроб, а невизначеність в цілому задачі для даного розв'язуючого алгоритму

$$N(A) = \sum_i p(m_i) \log \overline{K}(m_i). , \tag{7}$$

Якщо до спроби задача мала для заданого розв'язуючого алгоритму невизначеність N_0, а після спроби –

невизначеність N_1, то кількість одержаної корисної інформації $I_к = N_0 - N_1$. Якщо ймовірності $p(m_1)$ фіксовані і відомі, то невизначеність задачі дорівнює ентропії розподілу ймовірності вирішень. Незнання ймовірностей приводить до збільшення невизначеності.

IV Окремі моделі цінності інформації

Цінність інформації може по різному змінюватись внаслідок виконання деяких операцій над нею, приміром реалізації загроз. З практичної точки зору важливі, перш за все економічні наслідки, які виражаються як втрати або збитки. В основі теорії цінності інформації лежить уявлення про цінність інформації, заданої у вигляді таблиці її значень при різних сполученнях змінних, від яких ця цінність залежить. По аналогії введемо функцію втрат у вигляді сукупності можливих значень множини параметрів, які можна уявити сукупністю відображаючих точок у багатомірному просторі, тобто функції (або вектора, координатами якого є змінні, від яких залежить цінність цієї інформації)

$$R(I) = F(I, t, Con, Int, Av, Ac), \quad (8)$$

де I – кількість інформації; t – час; Con – показник конфіденційності інформації; Int – її цілісності; Av – доступності; Ac – спостережності. Задача комплексної системи інформаційної безпеки зводиться до підтримання рівня цінності інформації при різних сполученнях змінних. Далі розглянемо окремі моделі цінності в проекції вектора цінності на вказані у співвідношенні (8) осі координат.

Залежність цінності інформації від її обсягу I. Цінність інформації залежить від її обсягу (кількості). Інформація має тенденцію до збільшення конфіденційності, а значить і цінності з ростом її кількості. Приміром технологічна інформація в базі даних АТС має певну цінність. Та ж інформація в базі даних міської цифрової мережі, будучи семантично зв'язаною з інформацією щодо інших АТС, має більшу питому цінність $z = Z/I$. Відомий спосіб підвищення захищеності документальної інформації при її передаванні чи транспортуванні полягає у розділенні секрету – інформація поділяється на частини і передається незалежними маршрутами. Сума секретів частин менша за секрет повної інформації.

Дана залежність є відображенням ієрархічної багаторівневої (багатошарової) природи систем. З підвищенням рівня складності виникають нові властивості об'єктів. На кожному рівні об'єкти (послуги) формуються з об'єктів нижнього рівня. При цьому, при об'єднанні необхідним способом об'єктів нижнього рівня, приміром транзисторів чи інтегральних схем, на верхньому рівні виникає об'єкт (блок чи пристрій), який має нові властивості, які були відсутні у множині складових об'єктів нижнього рівня. Нові властивості означають виникнення нової інформації за рахунок опрацювання старої. Ентропія множини об'єднаних об'єктів, поставлених у певну залежність, змінюється. Закон збереження інформації при цьому не порушується. Ентропія об'єднання двох систем менша суми індивідуальних ентропій на взаємну інформацію, яка міститься у кожній з систем відносно іншої системи

$$H(XY) = H(X) + H(Y) - I(Y, X), \quad (9)$$

де $I(Y, X)$ – інформація, яка міститься у множині Y відносно множини X, тобто кількість інформації $I(Y, X)$ вимірюється зменшенням степені невизначеності множини X, яке виникає в результаті зняття невизначеності зв'язаної з ним множини Y.

Нова інформація виникає за рахунок "знищення", точніше за рахунок опрацювання інформації нижнього рівня. Несуттєва інформація нижнього рівня на вищому рівні вже не використовується. Завдяки зменшенню ентропії при об'єднанні елементів систем на вищих рівнях людина може вивчати, створювати і використовувати дуже складні системи. При цьому менша кількість інформації на вищих рівнях має більшу питому цінність, бо можливі втрати від її компрометації більш високі. Ентропія змінюється за рахунок того, що у об'єднаній системі об'єкти нижнього рівня зв'язуються між собою, сумарне число їх станів зменшується за рахунок кореляційних і/або функціональних зв'язків. Приміром, стани транзисторів у схемі тригера залежать один від одного. Якщо один транзистор відкритий, то другий - закритий внаслідок дії зворотних зв'язків. Число станів тригера менше, ніж загальне число станів ізольованих транзисторів, що його утворюють. Але триггер як перетворювач сигналів має нові функціональні можливості, інше число входів і виходів, інше число станів.

У нормативних документах сфери технічного захисту інформації (ТЗІ) [11], інформація в локальних обчислювальних мережах (ЛОМ) за рівнем інтеграції поділяється на сукупність сильно пов'язаних об'єктів, які потребують забезпечування своєї цілісності як сукупність, або окремі слабко пов'язані об'єкти, які мають широкий спектр способів свого подання, зберігання й передавання і потребують забезпечення власної цілісності кожен окремо.

Сильно пов'язані об'єкти – це сукупність наборів даних з мінімальною надлишковістю, які припускають їхнє оптимальне використання одним чи декількома процесами як водночас, так і в різні проміжки часу й потребують безумовного забезпечення цілісності цих наборів даних як сукупності. Прикладами сильно пов'язаних об'єктів можуть бути бази даних, які підтримуються для галузі системами

керування або сукупності наборів даних, які генеруються й модифікуються будь-якими функціональними чи системними процесами, і кожен з наборів даних не може самостійно опрацьовуватись, зберігатися й передаватися.

Слабко пов'язані об'єкти – це відносно незалежні набори даних, які генеруються, модифікуються, зберігаються й опрацьовуються в автоматизованій системі. Слабко пов'язані об'єкти – це інформаційні структури, подані у вигляді окремих файлів, котрі підтримуються штатними операційними системами робочих станцій та серверів, і кожний з них може опрацьовуватися, зберігатися й передаватися як самостійний об'єкт. Питома цінність сильно пов'язаних об'єктів більша і вимоги до їх захисту та технології опрацювання інформації більш сильні. Приміром, КСЗІ має реалізовувати механізми, що забезпечують фізичну цілісність як окремих складових сильно пов'язаних об'єктів, так і підтримання логічної цілісності сильно пов'язаних об'єктів, розосереджених в різних компонентах ЛОМ.

Зокрема, при накопичуванні інформації, яка підлягає видаленню, слід враховувати ефект акумуляції. Велика кількість несекретної інформації може стати більш конфіденційною, ніж мала кількість секретної інформації.

В деяких сферах модель залежності цінності інформації від її обсягу складніша. Так, існує суперечність між соціальною та індивідуальною потребою в інформації. З підвищенням рівня інформатизації соціальна потреба зростає. Але починаючи з деякого рівня необхідність у розширенні спілкування зменшується. Індивід утомлюється від інформаційного перенавантаження, що приводить відповідно до зменшення цінності інформації, тобто до зменшення очікуваного ефекту впливу.

Залежність цінності інформації від часу t. Дані залежності описують процеси старіння інформації, зокрема під час передавання повідомлень. Процес старіння полягає у тому, що цінність інформації, якщо її виражати в економічних показниках або в показниках ефективності, з плином часу, як правло, зменшується. Наступає момент, коли дане повідомлення вже не може бут використане для управління чи виробництва.

Інформація поділяється на інформацію з обмеженим життєвим циклом та інформацію з необмеженим життєвим циклом В нормативних документах сфери ТЗІ (у ЛОМ) розрізняють інформацію, яка за часом існування та функціонування є або швидко змінюваною з відносно коротким терміном її актуальності, або має відносно тривалий час існування за високого ступеня інтеграції й гарантування стану її незруйновності за умови приналежності до різних користувачів, в рамках сильно чи слабко пов'язаних об'єктів. До швидко змінюваної інформації з обмеженим життєвим циклом, перш за все, відноситься інформація керування. Реакція керуємої системи і керуючі впливи мають точно синхронізуватись.

Відповідно до своєї цінності інформація і вихідні дані системи, яка підтримує цю інформацію, можуть отримувати мітку рівня цінності або секретності і відповідно цієї мітки забезпечується певний рівень захищеності. На практиці інформація старіє і має певний період T життєвого циклу (рис. 1а), після якого інформація має бути утилізована тим чи іншим способом.

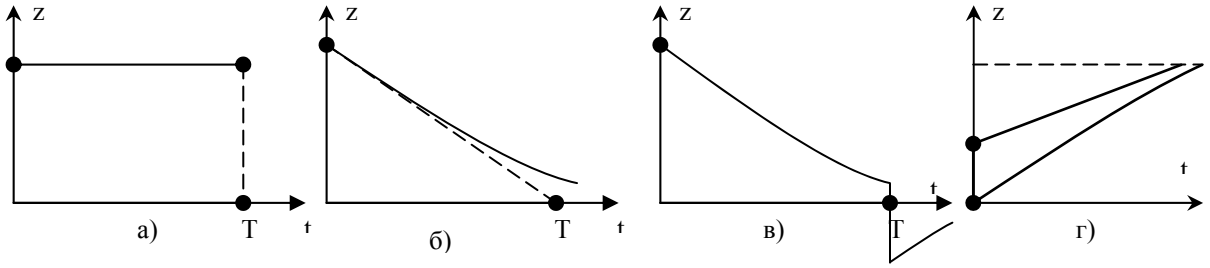

Рисунок 1 – Динаміка старіння інформації

Більшість процесів старіння можна описати експоненційною функцією (рис. 1б), $z(t) = 1 - e^{-Vt}$, де V – інтенсивність старіння, а середній час старіння $T = 1/V$.

Життєвий цикл інформації деякого роду має ту властивість, що по закінченню життєвого циклу цінність інформації може міняти знак. Її подальше застосування може приводити до негативних результатів (рис. 1г). Приміром, сигнал управління, затриманий більше норми, може не співпадати з фазою процесу, що регулюється, і приводити до так званого "розрегулювання" – збільшення помилки регулювання.

Цінність певних видів інформації може з часом збільшуватись. Це стосується перш за все науково-технічної інформації незалежно від того, чи є наукові уявлення вірними. Так зване "моральне старіння" у даному випадку є процесом порівняльного аналізу науково-технічної інформації та застосування на

практиці нових знань, а не обезцінювання попередніх, оскільки часто на їх основі виникають нові знання. З моменту виникнення науково-технічної інформації її цінність збільшується (рис. 1д) в міру збільшення числа фахівців, що з нею ознайомились, підтвердили її вірність або застосували на практиці. Початкова цінність може виникати, коли приймається рішення щодо досліджень чи публікації результатів.

Залежність цінності інформації від показників конфіденційності, доступності та цілісності. Як вже зазначалось, показники захищеності не є атрибутивними властивостями інформації. Показники конфіденційності, цілісності, доступності призначаються власником інформації у вигляді відповідних грифів, міток тощо. Для забезпечення призначеного рівня захищеності КСЗІ має реалізувати відповідні профілі захищеності та підтримувати призначені рівні секретності. На цьому етапі має значення відповідність призначеного рівня захищеності інформації та рівня цінності інформації. В одних випадках цінність інформації вище, якщо вона конфіденційна, в інших навпаки – за результатами застосування інформація більш цінна, коли вона більш відкрита і доступна. Ці залежності ще чекають свого детального дослідження. В усякому разі, коли рівень захищеності інформації завищено порівняно з її цінністю, виникають втрати у вигляді нераціонального збільшення витрат на її захист. Коли рівень захищеності занижений, можуть виникати втрати внаслідок витоку інформації або несанкціонованого доступу.

В процесі життєвого циклу захищеність інформації може змінюватись з часом, з виконаними операціями, зі способом зберігання, з функціонуванням КСЗІ, з цільовим призначенням інформації. Часто інформація перестає бути конфіденційною через деякий проміжок часу, наприклад, коли вона стає загальнодоступною (рис. 2а). Важливо, щоб весь час витримувалось оптимальне співвідношення між рівнем захищеності, що забезпечується КСЗІ, і рівнем цінності інформації. В зв'язку з цим, доцільно ввести показники конфіденційності k, які приймають значення між +1 та –1. Позитивна конфіденційність вводиться як міра необхідної закритості інформації, а негативна конфіденційність – як міра доцільної відкритості інформації.

Розглянемо приклад. Нехай деяка інформація готується до опублікування протягом інтервалу часу від t_0 до t_1. Якщо в цей час єдиний примірник документа буде викрадено, то будуть втрати на відновлення та від інших наслідків. Інформації слід призначити позитивний рівень конфіденційності і тим більший, чим більший об'єм інформації. Коли інформація підготовлена за час від t_1 до моменту власне публікації t_2 інформація старіє. Далі, якщо після опублікування зловмисник скопіював опублікований матеріал, то він, так би мовити, безкоштовно розповсюджує цей документ в інтересах видавника. Конфіденційність міняє знак, бо втрати тепер будуть, якщо виникнуть перешкоди у розповсюдженні документа.

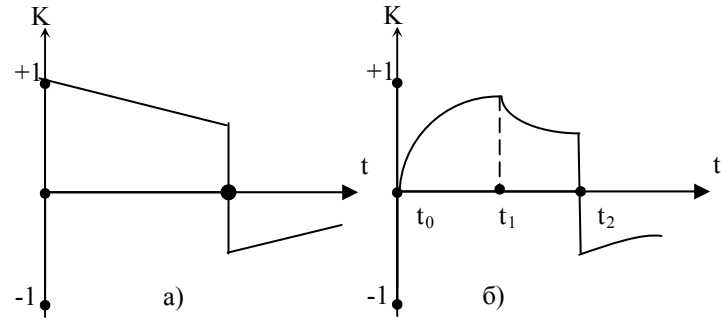

Рисунок 2 – Приклади зміни показника конфіденційності з часом

Цінність інформації залежить від її доступності. Доступність в свою чергу залежить від співвідношення швидкості передавання інформації і пропускної здатності телекомунікаційної системи, тобто від апаратної і алгоритмічної достатності телекомунікаційної системи. Методологічною основою аналізу затримки інформації та ймовірності її блокування при наявності лише техногенних та природних чинників загроз є теорія масового обслуговування.

Цінність інформації залежить також від її цілісності. Модель для оцінки цілісності інформації при передаванні через незахищене середовище в деяких радіосистемах без врахування антропогенних чинників загроз розглянута в [12].

Висновки

Проаналізовані відомі підходи до визначення цінності інформації, запропоновано багатокритеріальну оцінку цінності інформації як функцію, що залежить від властивостей інформації з позиції захисту. Приведені деякі з моделей цінності інформації залежно від показників обсягу, часу, конфіденційності,

доступності, цілісності.

Виходячи з принципу розумної достатності заходів захисту важливо далі вирішити проблему обчислення відвернутих втрат або шкоди, яку вдалося запобігти. З іншого боку, в теоретико-інформаційних підходах розвинуті напрямки врахування мети використання інформації та оцінки цінності інформації. Уявляються доцільними інтерпретації цих результатів для систем, в яких важливою є інформаційна безпека.

Напрямом подальшої роботи може бути дослідження властивостей моделей цінності інформації та застосування їх при проектуванні систем інформаційної безпеки телекомунікацій.

*Література: **1**. Сяо Д., Керр Д., Мэдник С., Защита ЭВМ: Пер. с англ. – М.: Мир, 1982. – 264 с. **2.** Кабелев Д., Князев А., Ловцов Д. Теоретико-концептуальный подход к проблеме качества и ценности информации в эргасистеме. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 7, 2003. С 25-31. **3**. Матов О. Я., Василенко В. С., Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах. // Реєстрація, зберігання і обробка даних. − 2004. − Т. 6, № 2. − С. 62 – 74. **4**. Воробиенко П., Нечипорук О, Щербина Ю. Принципы построения моделей угроз информационным ресурсам систем и сетей связи. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 7, К: 2003. С 11 – 13. **5**. Гайворонский С. А. Закон сохранения информации. http://www.gaivoronsky.narod.ru. **6**. Коган И. М. Прикладная теория информации. – М.: Радио и связь, 1981. – 216 с. **7**. Стратонович Р. Л. Теория информации. – М.: Сов. Радио. 1975. – 424 с. **8**. Solomonov R.J. A formal theory of inductive inference – Information and Control, 1964, V. 7, № 1. **9**. Шилейко А.В. Кочнев В. Ф., Химушкн Ф. Ф. Введение в информационную теорю систем / Под ред А. В. Шилейко. – М.: Радио и связь, 1985. – 280 с. **10**. Бонгард М. М. Проблема узнавания. М.: Наука, 1967, – 320 с. **11**. НД ТЗІ 2.5-008-2002. Вимоги з захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. **12**. Корнейко О., Кувшинов О, Лівенцев С. Метод захисту цілісності інформації, що передається в системах абонентського радіо доступу спеціального призначення. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 4, К: 2002. С 60 – 66.*

УДК 681.3.06

МЕТОДИКА ВИЗНАЧЕННЯ ДУМОК ЕКСПЕРТІВ ВІДНОСНО ЗРІЛОСТІ БЕЗПЕКИ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ МАТЕМАТИЧНОГО АПАРАТУ СУБ'ЄКТИВНОЇ ЛОГІКИ

Олександр Потій, Анатолій Лєншин

АТ „Інститут інформаційних технологій"

Анотація: **Обґрунтовано можливість використання апарату суб'єктивної логіки для оцінки зрілості систем забезпечення безпеки інформації. Розглядаються алгоритми формування думок у просторі суб'єктивної логіки. Пропонується новий метод, заснований на використанні зон базових думок, та обговорюються особливості його застосування.**

Summary: **Using possibility of this mechanism in information security system maturity level evaluating is given. Opinion forming method in space of Subjective Logic is described. New method based on using basis opinion regions is proposed and features of its application are considered.**

Ключові слова: **Інформаційна безпека, суб'єктивна логіка, збір знань, математичний апарат, зона базових думок.**

Вступ

На сучасному етапі розвитку комплексних систем захисту інформації в інформаційно-телекомунікаційних системах (ІТС) важливою задачею є проведення оцінки рівня захищеності ІТС. У сучасній практиці існує декілька підходів до оцінки рівня захищеності: аудит безпеки [1], розрахунок метрик безпеки [2], оцінка на основі використання моделі зрілості [3 – 6], підходи на основі оцінки ризиків тощо. Як міжнародні, так і національні органи ряду країн зі стандартизації розробляють документи, які мають надати методичну допомогу в роведенні такої оцінки [1 – 3, 6].

Одним із таких стандартів, у якому викладено методику проведення самооцінки, є документ Національного інституту із стандартизації та технологій США – NIST SP 800-26, який дозволяє провести комплексну оцінку захищеності в адміністративній, процедурній та програмно-технічній сферах