мережу для боротьби зі злочинами у сфері комп'ютерних технологій держав Великої вісімки (G-8) та інших країн (формату «24/7»));

11) покращити матеріально-технічне забезпечення підрозділів СБ України і МВС України, що здійснюють діяльність з протидії комп'ютерному тероризму та кіберзлочинності.

III Висновки

Комп'ютерний тероризм, як різновид технологічного тероризму, є новою формою терористичної діяльності, що на сучасному етапі становить загрозу національній та міжнародній безпеці. Загальнодержавна система протидії комп'ютерному тероризму має бути достатньо універсальною й здатною запобігати терористичним загрозам в інформаційній сфері України будь-якої природи, масштабів і динаміки та адекватно реагувати на їх виникнення. Запобігання є пріоритетним напрямом протидії комп'ютерному тероризму, складовими якої мають стати: приведення вітчизняного законодавства у відповідність до сучасного рівня розвитку інформаційних технологій; організація взаємодії та координація зусиль спецслужб, правоохоронних та судових органів, забезпечення їх необхідною матеріально-технічною базою; активізація міжнародного співробітництва у цій сфері.

Література: ***1.*** *Новий тлумачний словник української мови. У трьох томах / Уклад. В. Яременко, О. Сліпушко. - Т.3 «П – Я». Вид. 2-ге виправлене. – К.: «Вид-во АКОНІТ», 2006. – 862 с.* ***2.*** *Абсаментон С. К. Сучасний тероризм та проблеми забезпечення національної безпеки Республіки Казахстан. – Павлодар, 2000. - С.6.* ***3.*** *Беляков К. І, Цимбалюк В. С. Інформаційні технології як чинник терористичного акту // Боротьба з організованою злочинністю і корупцією (теорія і практика). Науково-практичний журнал. – 2003. - № 8. - С. 89-96.* ***4.*** *Тропинина Т. Киберпреступность и кибертерроризм // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 76-81.* ***5.*** *Голубєв В. Электронный терроризм - новое лицо терроризма // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 49-56.* ***6.*** *Голубєв В. А. Кибертерроризм - угроза национальной безопасности и интересам Украины // Юридичний журнал. - 2004. - №1. – С. 132-134.* ***7.*** *Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001 г.: оценка угроз и предложения по их нейтрализации // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. - Запорожье: Центр исследований компьютерной преступности. – 2004. - Вып.1. - С. 56-75.* ***8.*** *Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм // Боротьба з організованою злочинністю і корупцією (теборія і практика). Науково-практичний журнал. – 2007. - №17. – С. 316-324.*

УДК 519.724.681

ПРО ДЕЯКІ АСПЕКТИ ВИЗНАЧЕННЯ ЦІННОСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Олександр Архипов

Національний технічний університет України «Київський політехнічний інститут»

Анотація: **Розглянуто особливості визначення цінності конфіденційної інформації, зокрема, з урахуванням процесів старіння та фрагментації інформаційного ресурсу на окремі блоки. Наведено структуру моделей цінності інформації.**

Annotation: **It is considered the features of determination of confidential information value, taking into account senescence and fragmentation processes of informative resource in particular. The structures of information value models are resulted.**

Ключові слова: **Цінність інформації, корисність інформації, важливість інформації, збитки, модель цінності інформації, фрагментація інформації** .

I Вступ

Сфера захисту секретної інформації набула системних ознак на рубежі 19 – 20 століть [1]. Головними чинниками її формування були інтуїція та досвід професіоналів, які опановували цю сферу. Порівняно з охороною державної таємниці галузь технічного захисту інформації (ТЗІ) системно сформувалася пізніше, у другій половині 20-го століття, а в Україні утворення системи ТЗІ фактично співпало з становленням її незалежності. Характерною ознакою формування вітчизняної системи ТЗІ була наявність вже достатньо

розвиненої науково-методичної бази, що мало б сприяти формуванню основних науково-методичних засад системи ТЗІ ще на етапі її становлення. На практиці ж ряд базових науково-методичних положень захисту інформації ще й досі потребує своєї розробки або суттєвого уточнення. Зокрема, це стосується поняття цінності конфіденційної інформації.

Одним з базових положень побудови систем захисту інформації (СЗІ) є принцип розумної достатності, відповідно до якого витрати на побудову та супровід СЗІ мають співставлятися з можливими втратами, обумовленими реалізаціями загроз щодо інформації, яка підлягає захисту. Це дозволяє оптимізувати витрати на створення СЗІ, забезпечивши адекватність рівня захисту рівню цінності інформації. Тому визначення кількісного значення цінності інформації, яку треба захищати, є провідним моментом процедури оптимізації витрат на СЗІ [2]. Дещо конкретніше це положення сформульовано в [3]: "Захисту підлягає не будь-яка інформація, а тільки та, що має цінність. Цінною стає інформація, володіння якою дозволяє отримати який-небудь виграш: моральний, матеріальний, політичний тощо... Цінність інформації є критерієм прийняття будь-якого рішення про її захист". Зміст цього фрагменту достатньо переконливий щодо актуальності та важливості застосування поняття цінності інформації для побудови та оптимізації СЗІ, однак саме поняття "цінність інформації" залишається фактично не визначеним.

Слід зазначити, що наразі немає єдиного нормативного тлумачення терміну "цінність інформації", більш того, часто його визначення мають своєрідний непрямий, опосередкований характер. В посібнику з інформатики [4] маємо: "цінність інформації проявляється в тому випадку, коли вона сприяє досягненню мети, поставленою перед споживачем", в іншому посібнику [5] читаємо: "цінність будь-якого джерела інформації визначається як різниця між корисностями двох оптимальних стратегій, одна з яких забезпечує можливість вільного вибору різних дій при отриманні наслідків, пов'язаних з використанням інформації, а інша – при відсутності такої можливості". Поважне академічне видання [6] розуміє цінність інформації як "властивість, що визначається її придатністю до практичного застосування в різних галузях цілеспрямованої людської діяльності для досягнення певної мети". Близькі до наведеного, хоча і дещо змінені, звужені за змістом пояснення терміну " цінність інформації" надаються в [7, 8].

Головним питанням практичного застосування цінності інформації є знаходження (обчислення) кількісної оцінки цінності інформації. Ця проблема має давню історію, її дослідженню присвячена величезна кількість публікацій, зокрема, класичні для цієї галузі роботи К. Шеннона, О. О. Харкевича, Р. Л. Стратановича, М. М. Бонгарда та ін. [9 – 12]. Аналіз наведених в літературних джерелах результатів дозволяє стверджувати, що існуюче різноманіття підходів та методів визначення цінності інформації об'єктивно обумовлено існуванням різних видів інформаційних систем, де оброблюється чи циркулює оцінювана інформація, множиною неспівпадаючих цілей, щодо реалізації яких використовується ця інформація, особливостями прикладних задач, до розв'язку яких вона застосовується.

II Постановка задачі

Значення рівнів цінності інформації не можуть бути отримані шляхом прямого вимірювання, бо цінність інформації являє собою так звану латентну (приховану) властивість, яка є неспостережною й невимірною безпосередньо, оскільки до неї незастосовна процедура вимірювання еталонною одиницею. Для вимірювання латентної властивості необхідно виразити її через вимірювані властивості, які отримали назву індикаторів. Сукупність індикаторів, що замінює латентну властивість (змінну), утворює операціональний референт [14] або операціональний конструкт. Він використовується замість латентної змінної в усіх залежностях, в які вона входить. Операціональний конструкт має бути достатньо валідним відносно своєї латентної змінної, тобто має достатньо точно відтворювати її властивості, критичні для всіх застосувань, де задіяна латентна змінна.

В найпростішому випадку операціональним конструктом може бути окремий індикатор, зокрема, для латентної змінної "цінність інформації" ним може бути придатність інформації до практичного застосування. В цьому разі спосіб вимірювання значень обраного індикатора залежить від мети використання інформації у кожному конкретному практичному застосуванні, що в кінцевому підсумку й обумовлює появу множини підходів і методів оцінювання рівнів індикаторів.

Якщо як індикатор латентної змінної "цінність інформації" взяти корисність використання інформації в різних прикладних застосуваннях, та як одну з головних вимог визначити необхідність грошової форми представлення значень цього індикатора, отримаємо достатньо універсальний операціональний конструкт, незалежний від способу "вимірювання" (обчислення) рівня корисності в кожному конкретному застосуванні. Мається на увазі, що при оцінюванні рівня корисності, обумовленої зростанням ефективності виконання несхожих прикладних завдань завдяки використанню певної допоміжної інформації, припустиме застосування відповідних не співпадаючих способів обчислення цієї корисності. Головне – щоб ці оцінки були обчислені в єдиній шкалі, що забезпечує можливість їх наступного порівняння та сумісного

дослідження. Зауважимо, що аналіз літературних джерел, зокрема наведених вище [9 – 12], дозволяє констатувати, що в більшості випадків оцінювання цінності інформації, за умов дотримання певних додаткових вимог, зводиться саме до оцінювання корисності прикладних застосувань цієї інформації. Це дозволяє сформулювати наступне положення: цінність інформації вимірюється рівнем максимальної корисності, отриманої від залучення оцінюваної інформації до оптимізації виконання певного завдання (виконання роботи, розв'язання задач та проблемних ситуацій, оптимізації параметрів виробничого процесу тощо) за умови найліпшого способу використання цієї інформації. Деякий екстремізм цього твердження, що його вносять звороти "максимальна користь", "найліпший спосіб використання", отримав назву принципу (умов) екстремальності. Очевидно, що якість конкретного прикладного застосування інформації може бути різною. Відтак корисність цієї інформації може змінюватися в широких межах. Дотримання принципу екстремальності гарантує найвищу якість використання інформації, відповідно найвищу (максимальну) корисність її застосування. Кількісна оцінка цієї максимальної корисності визначає цінність інформації. Тобто, саме наявність принципу екстремальності в наведеному тлумаченні цінності інформації є запорукою коректного однозначного кількісного визначення цінності.

III Моделі цінності інформації

Формально цінність інформації можна відповідно до викладеного вище визначити наступним чином:

$$V(I) = \Delta A_{extr}(I) - d(I), \tag{1}$$

де A – показник, що характеризує ступінь успішності виконання певного завдання, роботи, іншого виду діяльності (цим показником може бути вартість продукції, виготовленої за певний час чи з фіксованого обсягу вихідної сировини, виграш, обумовлений вибором вдалого рішення, загальна вартість послуг, наданих споживачам у певній сфері діяльності тощо);

$d(I)$ – витрати на одержання, обробку та використання інформації I у певному виді діяльності;

ΔA – покращення (зростання) показника A за рахунок отриманої інформації I:

$$\Delta A(I) = A(I) - A_0, \tag{2}$$

де A_0 – вихідне значення показника (за відсутністю інформації I), $A(I)$ – збільшене завдяки використанню інформації I значення показника A. Зокрема, значення A може збільшитись внаслідок застосування отриманої інформації для оптимізації параметрів виробничого процесу, зменшення можливих хибних або неперспективних варіантів рішення певної проблеми, зростання іміджевої привабливості даного виду професійної діяльності й т. п.

Дотримання принципу екстремальності обумовлює зростання показника A до його максимально можливого значення A_{extr}, то ж

$$\Delta A_{extr}(I) = A_{extr}(I) - A_0. \tag{3}$$

У кожному конкретному застосуванні інформації I спосіб її "споживання" буде різним: разове використання інформації I у задачах прийняття рішення для вибору найкращого рішення з множини можливих; розподілене в часі поточне використання інформації для налаштування параметрів виробничих процесів тощо. Очевидно, що найбільш прийнятна форма виміру значень V, A, d – грошова, хоча на практиці використовуються умовні одиниці, бали та інше. Крім того, у більшості випадків величини V, A, d носять детермінований характер і їх значення можуть бути точно обчислені за існуючими нормативами та тарифами (виключення становить задача прийняття рішення на множині варіантів з відомою інформацією про розподіл ймовірностей їх реалізацій). Зазначимо, що наведений спосіб обчислення рівня корисності інформації, як і більшість традиційних методів та підходів до визначення цінності інформації, базуються на парадигмі позитивності наслідків залучення інформації до оптимізації певних видів робіт (прийняття рішень, розв'язання задач, виконання завдань). Однак в задачах захисту інформації (ЗІ) ця парадигма не спрацьовує, бо виникає відсутня раніше потреба в чіткому визначенні того суб'єкта інформаційних відносин (власника/споживача інформації чи зловмисника), для якого в цій ситуації визначається цінність інформації. Наприклад, для зловмисника несанкціонований доступ до конфіденційної інформації I, легітимне право на ознайомлення з якою у нього відсутнє, в більшості випадків стимулюється перспективою отримання певного прибутку, пов'язаного саме з використанням цієї конфіденційної інформації у своїх інтересах [15]. Тому для зловмисника корисність цієї інформації I очевидна. Що стосується власника/споживача інформації I, то тут ситуація має подвійний характер. По-перше, ця інформація може бути корисна в традиційному сенсі. По-

друге, компрометація інформації I здатна призвести до збитків, обсяг яких значно перевищуватиме корисність, визначену за співвідношенням (1). Це є достатнім мотивуванням необхідності захисту цієї інформації, отже в певному розумінні визначає цінність інформації I. Тому питання визначення цінності інформації, яка підлягає захисту, потребує додаткового розгляду.

Як відомо [7, 8] , споживчі якості інформації в повному обсязі гарантуються за умов забезпечення трьох властивостей інформації:

– доступності (можливості отримання санкціонованим користувачем потрібної йому інформації не пізніше заданого (малого) проміжку часу, захищеність її від несанкціонованого блокування) [18];

– цілісності (захищеність інформації від несанкціонованого знищення, модифікації) [18];

– конфіденційності (неможливість отримання інформації неавторизованим користувачем, захищеність від несанкціонованого ознайомлення) [18].

Розглянемо дещо детальніше ситуації, що виникають в разі реалізації загроз щодо трьох наведених властивостей інформації. Так, у випадку разового використання інформації I в задачі прийняття рішення, знищення або блокування цієї інформації обумовлює неможливість зростання показника A, тобто $\Delta A = 0$. Це означає, що споживач інформації задарма витратив гроші $d(I)$ на підготовку та обробку вчасно невикористаної інформації I. Додавши сюди втрачену вигоду, максимальний обсяг якої складає $\Delta A_{extr}(I)$, отримуємо граничний обсяг збитку споживача:

$$l = \Delta A_{extr}(I) + d(I). \tag{4}$$

У випадку використання поточно оновлюваної інформації, надходження якої розподілене у часі, її блокування чи знищення призведе практично до такого самого збитку, але з деяким часовим запізненням (лагом), впродовж якого збиток зростатиме від 0 до l.

У разі модифікації інформації, при невиявленні факту модифікації, збитки споживача інформації можуть сягати суттєвих значень, перевищуючи як $\Delta A(I)$, так і $A(I)$, та мають, на відміну від (4), імовірнісний характер.

Однак найбільші збитки характерні для випадку порушення конфіденційності інформації. При їх оцінюванні слід зважати на існування множини можливих сценаріїв розвитку подій [16], тобто ці збитки мають принципово імовірнісний характер. Крім того, в разі виявлення факту компрометації конфіденційної інформації, до загального обсягу збитків слід додати витрати на відновлювальні роботи, пов'язані з ліквідацією наслідків компрометації інформації.

Загалом структура збитків, що їх несе власник/споживач конфіденційної інформації через її втрату, має чотири складові:

$$L(I) = l_1 + l_2 + l_3 + L_\Sigma(I), \tag{5}$$

де l_1 – витрати на створення та обробку конфіденційної інформації I (близькі або співпадають з $d(I)$),

l_2 – втрати можливого прибутку за рахунок використання конфіденційної інформації I (у ряді випадків співпадають з $\Delta A(I)$),

l_3 – витрати на створення та експлуатацію СЗІ,

$L_\Sigma(I)$ – інтегральна оцінка збитку, що є наслідком можливих результатів розвитку ряду негативних для власника/споживача сценаріїв подій, обумовлених втратою конфіденційної інформації [16].

Зазначимо, що складова l_2 у випадку, коли реалізація загрози інформації не веде до знищення чи спотворення інформації, що застосовується для оптимізації виконання певних завдань (а отже, ті виконуються в незмінних умовах), може бути відсутньою.

За своїм характером $l_1 - l_3$ – детерміновані величини, значення яких для діючої виробничої системи мають бути достеменно відомі. Складова $L_\Sigma(I)$ – імовірнісна величина, яка для свого обчислення вимагає знання пар $< p_j, L_j >$ – ймовірностей розвитку кожного з можливих сценаріїв та результуючих збитків за кожним з них. Зважаючи на те, що в разі недосконалості СЗІ власник конфіденційної інформації I може понести максимальний збиток в розмірі $L(I)$, саме ця величина приймається як цінність $V(I)$ конфіденційної інформації.

В семантичному розумінні найбільш адекватною реальній економічній ситуації, що наступає після здійснення загрози, буде структура, яка включає такі три складові:

– втрачена цінність;

– збитки, обумовлені модифікацією чи розголошенням конфіденційної інформації;

– витрати на отримання та зберігання інформації.

Відповідно до викладеного вище, остання складова включає в себе витрати l_1, l_3.

Доцільно більш детально розкрити зміст двох перших складових. Зокрема, обраховуючи втрачену цінність, зважатимемо на такі часткові показники:

а) корисність інформації як інформаційної складової забезпечення якості та ефективності певної діяльності;

б) "самостійну" корисність інформації з точки зору її необхідності для розв'язання ряду задач означеної вище діяльності.

Обчислення збитків теж базується на двох часткових показниках:

а) величині шкоди, обумовленої модифікацією чи розголошенням конфіденційної інформації;

б) витратах на проведення робіт з ліквідації наслідків розголошення конфіденційної інформації.

IV Врахування процесів старіння та фрагментації інформації при визначенні її цінності

Наведені вище модельні співвідношення базуються на доволі спрощеному підході до аналізу цінності інформації. Подальше поглиблення досліджень в цій сфері стикається з необхідністю розгляду та вивчення ряду проблемних питань. Наприклад відомо [5, 17], що цінність інформації, в тому числі і конфіденційної, змінюється з часом. Вважається, що домінуючою тут є стала тенденція зменшення цінності, яка дістала назву процесу старіння інформації. Вважається, що в більшості випадків адекватною моделлю процесів старіння є експоненційна функція виду

$$L(t) = L(0)(1 - e^{-\beta t}), \tag{6}$$

де $L(0)$ – початкова цінність інформації, коефіцієнт β – інтенсивність старіння інформації, $1/\beta$ – середній час старіння.

Ще однією важливою особливістю конфіденційної інформації є нелінійна залежність її цінності L від обсягу цієї інформації. Нехай повний обсяг $I_{\max}$ конфіденційної інформації є достатнім для успішної реалізації завдань певної прикладної галузі людської діяльності. Цінність цього обсягу конфіденційної інформації становить $L_{\max} = L(I_{\max})$. Якщо припустити, що певний фрагмент цієї інформації обсягом I потрапить до зловмисника, максимальний рівень збитку, який може бути нанесений власнику інформації, залежатиме від того, наскільки повно за цим фрагментом зловмисник в змозі відновити зміст всієї вихідної інформації $I_{\max}$. Якщо обсяг I близький до 0, відновити за цим фрагментом вихідну інформацію практично неможливо навіть у випадку, коли до цієї справи зловмисником залучається досвідчений і добре підготовлений аналітик. Відповідно цінність такого фрагменту дорівнює 0. Навпаки, якщо обсяг I близький до $I_{\max}$, цінність цього фрагменту фактично становить $L_{\max}$, бо дуже ймовірно, що фахівець-аналітик отримає всі необхідні для зловмисника відомості з наявного фрагменту інформації і цінність відсутньої інформації $\Delta I = I_{\max} - I$ буде нульовою. Приймаючи це до уваги, можна припустити, що залежність $L(I)$ – монотонно зростаюча на інтервалі $(0, I_{\max})$ функція, похідна якої дорівнює чи близька до 0 у початковій та прикінцевій області цього інтервалу, але інтенсивно зростає в його середній частині. Подібним вимогам задовольняє модель виду

$$L(I) = L_{\max}\left[1 - \frac{1}{\beta_2 + (1-\beta_2)e^{\beta_1 I}}\right], \tag{7}$$

де β_1, β_2 – коефіцієнти, для значень яких виконуються умови: $\beta_1, \beta_2 > 0$, $\beta_2 \le 1$. Графічно ілюстрацію залежності (7) наведено на рис. 1. Слід зазначити, що інтенсивність зростання змінної L залежить від рівня підготовки та інтелекту аналітика [2]. У моделі (7) це відображається вибором значень коефіцієнтів β_1, β_2: зростання значень β_1 зміщує початок підйому графіка $L(I)$ вліво, до області малих значень I, а тривалість "лінійної" частини графіка регулюється підбором значень β_2, зокрема зростає із зменшенням цих значень і є короткою для значень β_2, близьких до 1.

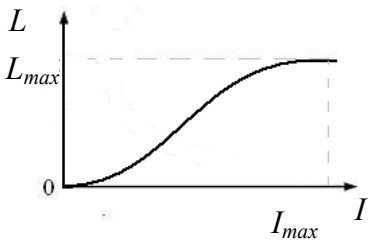

Рисунок 1 – Залежність цінності інформації від обсягу інформації

До речі, при недостатній фаховій обізнаності аналітика можлива ситуація, коли $L(I_{\max}) < L_{\max}$, причому різниця $L_{\max} - L(I_{\max}) = \Delta L$ є достатньо суттєвою.

Нажаль моделі (6), (7) дають лише загальне уявлення про вплив факторів часу та обсягу інформації на її цінність. Прикладне використання цих моделей, як і ряду інших специфічних модельних механізмів впливу різних факторів на цінність інформації [3, 17], потребує деталізації і адаптації відповідних моделей до умов і особливостей конкретних застосувань. На практиці це є вкрай проблематичним через недостатню дослідженість впливу означених факторів на цінність інформації, тому найбільш поширеним способом врахування подібних впливів є апарат експертного оцінювання.

V Інформація: цінність чи важливість?

Вище для кількісного оцінювання латентної змінної "цінність інформації" було введено операціональний конструкт, головну роль в якому відігравав індикатор "корисність інформації". У формальній моделі (1) значення цього індикатору визначалось через показник $\Delta A_{extr}(I)$ – максимальний приріст успішності виконання певного завдання. Однак у базовому співвідношенні (5), яке характеризує цінність конфіденційної інформації, індикаторами, що формують операціональний конструкт, стають збитки – антипод корисності. Цими індикаторами є витрати l_1, l_3, "чисті" збитки, які інтегрально представлені змінною $L_\Sigma(I)$, та збиток l_2 – втрачений прибуток, який доречно було б назвати "негативною (втраченою)" корисністю. В зв'язку з цим асоціювання узагальненого (сумарного) збитку $L(I)$ з поняттям "цінність інформації" є, зважаючи на первинну традиційну семантику цього поняття, не зовсім коректним. Можливо через це в деяких джерелах для узагальненої характеристики значимості інформації використовують термін "важливість інформації" [3, 19], або "значимість інформації" [21]. Зокрема в [22] маємо: "важливий – ... вартісний, цінний... 1) Який має велике, особливе значення...", в [23]: важливий – той, що має велике значення, від іменника waga (польск.) "вага, важкість", в переносному значенні "значимість", "цінність", тобто за своїм змістовним навантаженням "важливий" ширше за "цінний". Цікаво, що в законі України "Про державну таємницю" від 21. 09. 1999р. №1079-XIV для порівняльної характеристики властивостей секретної інформації застосовано термін "важливість" (його ж використано для позначення найвищого ступеня секретності – "особливої важливості").

VI Висновки

Проаналізовано відмінності підходу до визначення цінності конфіденційності інформації порівняно із традиційним підходом, що базується на парадигмі позитивності наслідків застосування інформації для підвищення ефективності різних видів діяльності. Запропоновано узагальнену структуру цінності конфіденційної інформації, розглянуто деякі особливості оцінювання цінності, пов'язані з процесом старіння інформації та фрагментацією її на окремі блоки.

*Література: **1**. Ботвінкін О. В. та ін. Історія охорони державної таємниці в Україні: монографія. – К.: Наук.-вид. відділ НА СБ України, 2008.-155с. **2.** Архипов О. Є., Ворожко В. П. Системні аспекти оцінювання рівня важливості секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., - 2007. – Вип. 2 (15). – с. 10-12. **3.** Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электроинформ, 1997. – 368с.:ил. **4.** Основы экономической информатики: Учеб. пособие / А. Н. Морозевич, Н. Н. Говядинова, Б. А. Железко и др.; Под общ. ред. А. Н. Морозевича.- Мн.: ООО "Мисанта", 1998. –438 с. **5.** Романов В. П. Интеллектуальные информационные системы в экономике.- М.: Издательство "Экзамен", 2003.- 496 с. **6.** Кондаков Н. И. Логический словарь – справочник. - М.: Наука, 1976.- 720 с. **7.** Богуш В. М., Юдин О. К. Інформаційна безпека держави. – К.: "МК-Прес", 2005.-432 с. **8.** Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД"ДС", 2001.-688 с. **9.** Циба В. Т. Математичні*

основи соціологічних досліджень: кваліметрічний підхід. – К.: МАУП, 2002.- 248 с. ***10.*** *Хайтун С. Д. Количественный анализ социальных явлений: проблемы и перспективы. – М.: КомКнига, 2005.- 280 с.* ***11.*** *Современное состояние теории исследования операций /Под ред. Н. Н. Моисеева. – М.: Наука, 1979. – 464 с.* ***12.*** *Харкевич А. А. О ценности информации.- Проблемы кибернетики, 1960, №4, с. 14-21.* ***13.*** *Стратанович Р. Л. О ценности информации.- Изв. АН СССР. Техническая кибернетика, 1965, № 5, с.3-12.* ***14.*** *Бонгард М. М. Проблемы узнавания. – М.: Наука, 1967. – 320 с.* ***15.*** *Архипов А. Е., Архипова С. А. Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе "атака-защита"// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., - 2008. – Вип.1 (16). – с.57-61.* ***16.*** *Архипов О. Є., Касперський І. П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. К., - 2007. – Вип. 2 (15). – с. 13-19.* ***17.*** *Ефимов А. Н. Информация: ценность, старение, рассеяние.- М.: Знание, 1978.- 64 с.* ***18.*** *НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***19.*** *Государственная тайна в Российской федерации / Под ред. М. А. Вуса – СПбГУ, 1999.- 330 с.* ***20.*** *Свиридов В. В. Контроль в сложных системах. М.: Знание, 1978. –64 с.* ***21.*** *Минаев Г. А. Безопасность организации. – К.: КНТ, 2009.- 440 с.* ***22.*** *Новий тлумачний словник української мови, т. 1 / Укладачі В. В. Яременко, О. М. Сліпушко –К.: Вид. "Аконіт", 2007.- 926 с.* ***23.*** *Цыганенко Г. П. Этимологический словарь русского языка .-К.: Рад. шк; 1989.- 511 с.*