**УДК 681.5:621.391**

# ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДКРИТИХ СИСТЕМ. Частина 1. МІРИ ІНФОРМАЦІЇ ТА ВЛАСТИВОСТІ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ВІДКРИТИХ СИСТЕМ

***Володимир Кононович, Тетяна Тардаскіна****

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

Анотація: **Аналізуються новітні науково-технічні досягнення в області інформатики, інформаційних технологій та виводяться основні принципи інформаційної безпеки відкритих систем, що характеризуються інтелектульним управлінням й активною взаємодією з іншими системами. Уточнюються поняття цінності інформації у відкритих системах.**

*Summary:* **The newest scientific-technical achievements in informatics, information technologies and main principles of information security open systems, which characterized intellectual management and active interaction with other systems, are analyzed. Define more precisely conception of information value in open systems.**

*Ключові слова:* **Інформаційна безпека, відкриті системи, ентропія, інформодинаміка, квантова інформатика, кількість інформації, парадигма інформаційної безпеки, цінність інформації.**

## I Вступ

Дане дослідження стосується сфери технічного захисту інформації та інформаційної безпеки систем, які об'єднуються під загальною назвою – інформаційні технології. У сферах виробництва, економіки, соціальних і політичних відносин інформація отримала статус ресурсу. Інформаційна безпека стала властивістю не тільки систем спеціального призначення, а й притаманною всім системам. Послуги інформаційної безпеки мають надаватись в усіх інформаційних та інформаційно-телекомунікаційних системах. Ряд законів [1, 2], нормативних документів [3] та розвиток в Україні систем електронного уряду, електронного документообігу, цифрового підпису, електронної торгівлі тощо *ставлять проблемну задачу* захисту відкритої інформації. У інформаційно-телекомунікаційних системах вирішуються задачі захисту державного інформаційного ресурсу, до якого, крім інформації, яка становить державну таємницю, та конфіденційної інформації, яка належить державі, входить і відкрита інформація, важлива для особи, суспільства та держави. У рамках проблеми захисту відкритої інформації поки що не вироблено науково-методичних основ системи інформаційної безпеки, що утруднює розвиток нормативно-законодавчої бази та практичних розробок. У свою чергу, недосконаліть методів оцінки цінності (важливості) інформації перешкоджає створенню доказово ефективних систем захисту інформації. З іншого боку, проблеми інформаційної безпеки загострюються слідом за стрімким розвитком самих інформаційних технологій, де останнім часом отримані важливі науково-технічні результати у напрямах: розробки теорії квантової інформації та створення квантових комп'ютерів на новій елементній базі [4]; розробки інформодинаміки та створення на базі її досягнень комп'ютерів з архітектурою інформодинамічного типу [5]; моделювання живого у машині та створення нейроінтелектуальних комп'ютерів, які мають аналогію в процесах обробки інформації живими організмами [6]. *Аналіз цих досягнень та публікацій* дозволяє по новому підійти до вирішення проблем захисту інформації у відкритих системах та переглянути оцінки цінності інформації, які розроблені у роботах К. Шенона, А. Колмогорова, Р. Стратоновича, А. Харкевича та інших.

В рамках теорії інформації вироблені теоретичні поняття цінності інформації, які вже досліджувались і авторами цієї роботи [7]. Але ці поняття страждають суб'єктивізмом, неоднозначністю і їх важко пристосувати до вирішення практичних задач. Діапазон оцінок простягається від цінності кількості інформації до вартості інформації і до, так званої, «семантичної» цінності інформації, хоча вона має досить штучний характер. Деякі автори заперечують доцільність категорії цінності інформації, подібно тому, як у фізиці безпредметно говорити про цінність енергії або маси. В області захисту інформації використовуються різноманітні методи оцінки цінності інформації: кількісні і якісні, аналітичні і експертні, вартісні і споживчі, нечіткі і стохастичні тощо. Ці оцінки також характеризуються неточністю, розмитістю, невизначеністю, суб'єктивізмом. Результати етапу оцінки споживчої і функціональної цінності інформації суттєво впливають на проектування і характеристики системи інформаційної безпеки. Спроба аналізу впливу останніх досягнень інформаційних технологій на вирішення проблем інформаційної безпеки є актуальною.

***Мета даної роботи:*** дослідити новітні досягнення у сферах розвитку комп'ютерної техніки та теорії відкритих систем з точки зору інформаційної безпеки, виробити науково-методичні основи системи інформаційної безпеки відкритих систем, для яких характерним є обмін та обробка потоків інформації у процесі взаємодії з іншими системами і середовищем функціонування, уточнити практичні аспекти теоретико-інформаційних методів оцінки кількості та цінності інформації стосовно інформаційної безпеки.

Поняття інформації зв'язано, насамперед, з функціонуванням систем і, зокрема, з функціонуванням складних, так званих відкритих систем. *Формулювання задач та методи досліджень* зводяться, в основному, до використання методології трьох напрямів загальної та абстрактної теорії систем, а також теорій цінності інформації. Загальна теорія систем охоплює дисципліни, які мають відношення до аналізу та синтезу систем. Абстрактна теорія систем узагальнює різні підходи до загальної теорії систем. Теорія систем розрізняється залежно від методів досліджень на теорії систем по М. Месаровичу і теорії систем по фон Берталанфі.

Перший напрямок – теорія систем по М. Месаровичу – склався в кінці п'ятидесятих років минулого століття [8]. Він веде випробуваним шляхом створення математичних та фізико-математичних теорій і апаратів моделювання об'єктів, складність яких визначається кількістю складових частин і видом їх математичного описання. Сюди включають як теорії, які вивчають системи в цілому (наприклад, теорія динамічних систем, теорія конечних автоматів, теорія алгоритмів, квантова інформатика), так і ті, які розглядають поведінку систем (теорії управління, адаптації, самоорганізації тощо). Вражаючим досягненням є те, що цей напрям знаходиться на порозі створення квантового комп'ютера.

Другий напрямок – теорія систем по фон Берталанфі – склався у кінці сорокових років минулого століття [9]. Цю теорію представляють як теорію описання будь-яких систем, де на першому місті стоїть ієрархічна класифікація систем і далі, кожен рівень ієрархії аналізується з використанням того апарату, того ступеня абстракції, які допустимі на даному рівні для досягнення конкретної цілі поточного дослідження. Системи представляються і спостерігаються за допомогою абстрактних і природних мов, а методологією цього напрямку є вивчення і порівняння систем, складність яких визначається їх власним відношенням до інформації. Цей напрям характеризується як програма досліджень незамкнутих систем, направлена на пошук методів доведення існування деяких рис живого в системах, починаючи з деякого рівня їх системної складності [5].

Третій напрямок сформувався за рахунок кібернетики як збірний напрямок, моделюючий живе у машині і орієнтований на створення теоретичного фундаменту та імітаційного моделювання систем штучного та живого інтелекту [6]. Напрямок орієнтований на нечіткі методи та інтерактивні засоби нової епохи всеохоплюючої інтелектуалізації, де системи штучного нейроінтелекту та комп'ютерних наставників людини будуть відтворювати як свідомі так і підсвідомі механізми творчого мислення людини. Аналіз цього напряму знаходиться, поки що, поза рамками даного дослідження.

## II Вплив квантової інформатики на проблеми інформаційної безпеки

Квантова інформатика є новою областю науки і технології, яка поєднує у собі розділи фізики, математики, кібернетики та інженерії, відповідає на питання, як інформація може бути використана у реальному, тобто квантовому світі, і з'ясовує роль фундаментальних законів фізики у процесах одержання, передачі і обробки інформації. Квантовий комп'ютер на сьогодні визначають як фізичний пристрій, який виконує логічні операції над квантовими станами шляхом унітарних перетворень зі зберіганням енергії, і який не порушує квантові суперпозиції у процесі обчислень [12]. Рівень розробки квантового комп'ютера поки що не дозволяє ставити вимоги до його інформаційної безпеки. Скоріше навпаки, мова йде про використання фундаментальних властивостей квантових об'єктів у сфері інформаційної безпеки.

Одним із застосувань квантової інформатики є криптографія. Уже розроблені й реалізовані алгоритми, які використовують властивості неклонованості та неможливості вимірювань квантових об'єктів без збурення. Основний виграш у квантових криптографічних протоколах полягає у тому, що факт підслуховування стає відомим для користувачів [13]. Іншим застосуванням квантового комп'ютера є те, що він може вирішити задачу факторизації за долі секунди. Неможливість виконання факторизації лежить у основі нині найбільш надійних методів шифрування, які використовуються у багатьох країнах для захисту електронних банківських рахунків. Коли буде побудована машина для квантової факторизації простих чисел – тобто розкладання довільного числа на прості множники – усі криптографічні системи типу RSA стануть зовсім непридатними.

Робота квантового комп'ютера може бути представлена як послідовність чотирьох операцій: «ЗАПИС» (приготування) початкового стану; «ОБЧИСЛЕННЯ», тобто унітарні перетворення початкових станів; «ВИВЕДЕННЯ» результату або вимірювання. Четвертою допоміжною операцією є «СКИДАННЯ», яке приводить регістри до основного стану. Операція обчислення виконується з квантовою інформацією, а

операції запису і виводу виконують перетворення інформації із класичної форми у квантову і навпаки.

На побутовій мові інформація – це деяке знання про об'єкт. Поняття інформації тісно зв'язане з поняттям ентропії. Чим більша інформація, тим менша ентропія. Інформаційна ентропія при комбінаторному підході визначена Р. Хартлі (див. формулу (2) в [7]). Інформаційна ентропія дорівнює мінімальному числу двійкових комірок, за допомогою яких можна записати якусь інформацію, вважаючи всі повідомлення рівноймовірними. При інформаційно-теоретичному підході точне визначення інформаційної ентропії дане К. Шеноном у 1948 році як зменшення невизначеності при виборі, наприклад, як кількість інформації, що міститься у повідомленні або сигналі (див. формулу (1) у [7]). Міра кількості інформації К. Шенона введена так, що задовольняється теорема складання ентропій: ентропія об'єднання незалежних систем дорівнює сумі індивідуальних ентропій систем.

Після К. Шенона поняття ентропії набуло широкого розповсюдження, їй стали надавати різний фізичний смисл та застосовувати до інших наук та областей діяльності людини. Дійсно, ентропія, як міра невизначеності (або ступеню недостатності) інформації про дійсний стан фізичної системи, залежно від умов, може інтерпретуватись по різному. У Шенона – це кількість бітів відкритого тексту, які необхідно відкрити у шифротексті, щоб узнати увесь текст, у термодинаміці і статистичній фізиці – це міра невпорядкованості макростану системи або її безпорядку, в теорії інформації – це міра різноманітності, складності і навіть новизни, у деяких теоріях – це міра перетворення можливості у дійсність тощо. В квантовій інформатиці вводиться ентропія фон Неймана квантового стану $\rho$ співвідношенням

$$S = -\sum_n \rho_n \ln \rho_n \,, \tag{1}$$

де $\rho$ – статистична матриця густини, яка повністю задає квантові стани; $n$ – загальне число із сукупності систем з певними ймовірностями можливих станів системи.

Ентропія фон Неймана співпадає, за деякими винятками, з ентропією К. Шенона. Шенонівська ентропія дає міру невизначеності, зв'язану з класичним розподілом ймовірностей. Квантові стани описуються схожим чином, тільки замість розподілу ймовірностей використовуються оператори густини. Різниця між ентропією фон Неймана та ентропією К. Шенона зв'язана з властивістю не клонованості не ортогональних квантових станів та так званою досяжною інформацією. Досяжна інформація показує, яку інформацію можна отримати про величину $X$ із її вимірювань, і є взаємною інформацією між $X$ і результатом вимірювання $Y$. Величина, яка може бути досягнута при будь-яких вимірюваннях квантових систем, задається границею А. Холево:

$$H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x) \,, \tag{2}$$

де $\rho = \sum_{\mathrm{x}} \mathrm{p_x} \rho_{\mathrm{x}}$ .

Величина, що фігурує у правій частині (2), одержала назву інформація (або кількість) А. Холево. Теорема про границю А. Холево показує, що неможливо достовірно визначити $X$, виходячи з результатів вимірювань $Y$. Границя А. Холево встановлює зв'язок, у вигляді нерівності, між ентропією фон Неймана квантового ансамблю і класичною взаємною Шенонівською інформацією.

За одиницю інформації $I$ приймають кількість інформації у достовірному повідомленні, апріорна ймовірність якого дорівнює ½. Ця одиниця отримала назву *біт* (binary digits). Якщо у формулі використовується натуральний логарифм, то одиниця кількості інформації називають *натом:* $H_{Bit} = 1.44\, H_{Nat}$. Фізичні принципи обробки інформації в квантових і класичних логічних елементах відрізняються. Логічні операції, які виконуються над квантовими об'єктами, проходять за іншими правилами, ніж у класичних обчислювальних процесах. Класична ідея про двійкову (бітову) логіку замінюється моделлю квантових бітів – дворівневих систем. Прикладами дворівневих систем є дворівневі атоми, атоми з різними ядерними або електронними спінами тощо. Тому на квантовому рівні як фундаментальну одиницю кількості інформації введено квантовий біт – *кубіт*. Одиничний кубіт представляє собою стан дворівневої системи. Кубіт - це когерентна суперпозиція двох розрізнюваних квантових станів, наприклад, поляризації фотона ($H$, $V$) два стани спіну електрона, внутрішні електронні стани індивідуального атому. Ентропія фон Неймана ансамблю є середнім числом кубітів, необхідних для кодування станів ансамблю за допомогою ідеальної кодуючої системи.

Сцілардом при вирішенні парадоксу Максвела було встановлено зв'язок між інформаційною ентропією і термодинамічною ентропією. Повчальним у вирішенні парадоксу Максвела є те, що інформацію неможливо одержати безплатно. За неї доводиться платити енергією, в результаті чого ентропія системи підвищується на величину, у крайньому випадку, рівну її пониженню за рахунок одержаної інформації. Повторимо ці міркування, слідом за [14]. Нехай заданий макроскопічний стан деякої замкнутої системи, тобто з певним ступенем точності вказані значення таких параметрів, як об'єм, тиск, температура,

хімічний склад тощо. Кожному макро стану системи відповідає набір мікро-станів. Також нехай у мікро-стані точно задані стани всіх часток, які входять у систему. Для будь-якої макросистеми при температурі вище абсолютного нуля число мікро-станів *W,* що відповідають даному макро стану, величезне. *W* називається статистичною вагою або термодинамічною ймовірністю даного макро стану. Згідно з основним постулатом статистичної фізики, всі *W* мікро-станів мають однакову ймовірність. Величина *W* безпосередньо зв'язана з ентропією. За формулою Планка-Больцмана

$$S = k \ln W, \qquad (3)$$

де *k* – розмірна постійна Больцмана, $k = 1{,}38 \quad 10^{-16}$ ерг/град або $3{,}31 \cdot 10^{-24}$ ео (ео – ентропійна одиниця, 1 ео = 1 кал/град). Розрахуємо далі, яку кількість інформації необхідно отримати про систему, що знаходиться у даному макро стані, щоб однозначно визначити її мікро стан. Інакше кажучи, якої кількості інформації не вистачає до повного опису системи у заданому макро стані. Нехай зроблено неможливе: визначений мікро-стан (вектори і швидкості руху всіх молекул газу). До визначення ймовірності того, що макроскопічна система знаходилась якраз у цьому мікро стані, була рівною $1/W$, а після визначення стала рівною одиниці. Одержана кількість інформації

$$I = -\log_2 \frac{1}{W} = \log_2 W \cdot \qquad (4)$$

Формули (3) і (4) співпадають з точністю до постійного розмірного множника. Величини *S* та *I* ідентичні. Щоб перейти від кількості інформації в бітах до ентропії в ентропійних одиницях, необхідно в (2) перейти від логарифма при основі 2 до натурального логарифму й помножити на *k*. Тоді маємо:

$$S(\text{ео}) = 2{,}3 \cdot 10^{-24}\, I\ (\text{біт}). \qquad (5)$$

Інформація (ентропія), як фізична величина, у певному смислі еквівалентна енергії. Розглянемо таку систему, як парова машина. Результатом її функціонування може бути виконання деякої механічної роботи, тобто перетворення енергії з одної форми в іншу. Процес перетворення має бути організований. Частина енергії використовується для управління за типом зворотного зв'язку. Положення поршня оцінюється і залежно від його положення переключаються клапани подачі пару. Зворотний зв'язок можна організувати за допомогою механічних пристроїв, а можна й за допомогою мікропроцесорної системи управління. Для передачі сигналу контуром зворотного зв'язку та на перетворення сигналу в управляючу дію необхідно затратити певну енергію. Інформація є деяким еквівалентом цієї енергії.

Знайдено, що для ідеального газу, який складається з одної молекули, робота при ізотермічному процесі визначається різницею ентропій: $W = T(S_2 - S_1)$, де *T* – температура газу. За рахунок зменшення ентропії можна виконувати роботу. Але другий закон термодинаміки забороняє одержання роботи лише за рахунок тепла. У навколишньому світі замість виконання роботи відбувається зміна інформації про частку. Процес зміни зменшує ентропію частки, переводячи її у не рівноважний стан та рівно на стільки ж збільшує інформацію про систему, точніше про частку. Іншими словами, маємо $S + I = const$. За другим началом термодинаміки за інформацію треба платити збільшенням ентропії $S_з$ зовнішньої системи, причому $\Delta S_з > I$.

Квантовий комп'ютер може бути описаний на мікроскопічному, мезоскопічному і макроскопічному рівнях. При описаннях системи з використанням величин, які характеризують у сукупності ці рівні, виявляються ряд закономірностей, таких як самоорганізація систем, виникнення нової інформації, поява семантики інформації, тобто смислу. Квантовий комп'ютер представляє собою систему такого роду, що на квантовому рівні її можна описувати як відкриту і як закриту систему. Як у відкритій системі на мікрорівні квантового комп'ютера проходить обмін інформацією між мікро рівнем та макрорівнем – перетворення квантової інформації у класичну і навпаки. Самі обчислення виконуються на мікро рівні і можуть описуватись як логічні зворотні операції квантової логіки у закритій системі, які не супроводжуються розсіюванням енергії.

Основні характеристики і складові частини процесу самоорганізації розглянемо слідом за роботами [6, 15]. Самоорганізація може проявлятись у вигляді спонтанної появи відносно стійких структур. Механізми самоорганізації відіграють значну роль у мікро, мезо і макро світі. Матерія і процеси суттєво структуровані. Усі системи мають певну структуру. Впорядкованість (структурованість) повсюдно розповсюджена. Для того, щоб у системі почалась самоорганізація, вона повинна бути підведена до межі стійкості. Виникає складна нелінійна фізична система з хаотичним типом руху, в якій можна виділити параметри порядку і нерівноважності. Параметри порядку, або управляючі параметри, називають параметрами над критичності. Ці параметри надаються ззовні. Нестійкість починається з деякого «натяку» («хінта») на появу майбутньої структури, невеликого збурення – біфуркації. Якщо є лише два варіанти переходу системи у наступний стан рівноваги, то на появу майбутньої нової структури досить лише одного біта інформації з числа параметрів порядку. По мірі збільшення зовнішнього параметра нерівноваженості до певного порогу відбувається реальне створення структури. Початкова симетрія

порушується: можна сказати, що відбувається самочинне або спонтанне порушення симетрії. Умовами виникнення явища самоорганізації є:

- наявність параметрів порядку зі своїм механізмом нестійкості; всесвітня структурованість матерії свідчить про безліч механізмів нестійкості, і зв'язаних з ними параметрів порядку, у навколишньому світі;
- система має бути відкритою, щоб хаотичний рух підтримувався довгий час за допомогою енергії від зовнішнього джерела;
- джерело енергії має поставляти енергію в досить упорядкованому вигляді: за термінологією Брилюена [10] – у систему повинна вприскуватись «негентропія», тобто ентропія з оберненим знаком;
- надлишкова енергія, тобто частина організованої енергії має розсіюватись у навколишньому просторі (перетворюватись у тепло); всередині системи весь час народжується ентропія, яка витікає потім з теплом у навколишнє середовище; із системи необхідно видаляти «шлак» із ентропії, яка заново народжується.

Для самоорганізації необхідні два елементи «живлення» – енергія і негентропія. Лише їх сума може забезпечити стаціонарну підтримку нової структури у нелінійній дисипативній системі. Образно кажучи в систему необхідно вводити ентропію з оберненим знаком – негентропію. Якщо ентропія – це міра безпорядку, то ентропія з оберненим знаком – негетропія – це міра впорядкованості. Для підтримання стаціонарного стану само організованої системи недостатньо просто відводити надлишкову ентропію: на вхід цієї системи необхідно подавати енергію. Енергія, що підводиться до системи, має бути більш організованою у порівнянні з теплом: ентропія на одиницю цієї енергії повинна бути меншою ніж $1/T_c$, де $T_c$ – температура навколишнього середовища – для самоорганізації досить невеликої частини енергії, тієї, яка відноситься до параметрів порядку. Для початку процесу самоорганізації в системі, яка близька до порогу нестійкості, досить невеликої зміни параметру порядку.

Найбільший загальний подив викликають спостереження дивної впорядкованості біологічних структур і процесів на всіх рівнях від макромолекул до людини. Навіть стверджується, що біологічна еволюція живого має анти ентропійний характер. Блюменфельд спробував оцінити зміни ентропії, пов'язані з виникненням біологічної організації [11]. Тіло людини складається приблизно з $10^{13}$ клітин. Якщо допустити, що серед них нема однакових і що відносне розташування клітин у тілі людини однозначне, то кількість інформації, необхідної для побудови такої єдиної структури є $I = \log_2 (10^{13}) \approx 10^{13} \log_2 10^{13} \approx 4\ 10^{14}$ біт. Тоді пониження ентропії при побудові організму людини із клітинок складає $\Delta S \approx 2 \cdot 10^{-24} \cdot 4 \cdot 10^{14} \approx 10^{-9}$ ео. Відомо, що при випарюванні грама води ентропія підвищується приблизно на 1 ео. Таким чином, пониження ентропії при переході від хаотично розташованих клітинок до організму людини чисельно дорівнює підвищенню ентропії при випарюванні $10^{-9}$ грам води. Більш детальні розрахунки показують, що впорядкованість біологічної організації людського тіла „коштує" 300 ео. Ці оцінки показують, що виникнення і ускладнення біологічної організації здійснюється практично „безкоштовно". Явище самоорганізації зв'язане з виникненням нової інформації. У закритих системах ентропія згідно з другим законом термодинаміки не убуває, вона або збільшується, або у граничному випадку залишається постійною. У відкритих системах завдяки самоорганізації ентропія понижується. Організованість матерії підвищується.

Поняття ентропії не зв'язані з поняттями цінності, наявності смислу, важливості чи практичного значення інформації. Між тим у рамках теорії самоорганізації починає розроблятись концепція інформації, яка включає семантику [15]. Ідея такого підходу полягає у відносній значимості сигналів, які є носіями інформації на фізичному рівні. Смисл сигналу можна приписати лише тоді, коли спостерігач прийме до уваги відгук того, хто прийняв цей сигнал. Стани динамічної системи описуються набором величин $q_j(t)$,які змінюються з часом. Усі величини можна об'єднати у вектор стану системи $\mathbf{q}(t) = [q_1(t), q_2(t), \ldots, q_N(t)]$. З часом вектор $\mathbf{q}$ прагне вийти на деякий атрактор, тобто на притягуючу нерухому точку. До отримання сигналу система знаходиться у початковому стані $\mathbf{q_0}$. Нехай прийнятий сигнал задає управляючий параметр $\alpha$ і початкове значення вектора $\mathbf{q_0}$. Після приймання сигналу система може перейти у новий атрактор. У процесі переходу можливі ситуації невизначеності, коли перехід до нового атрактора проходить неоднозначно. Наприклад, внаслідок прийому сигналу і залежно від флуктуацій система може перейти у одну з двох усталених точок. Сигнал приносить деяку неоднозначність, і ця неоднозначність знімається флуктуаціями системи. Інформація в системі збільшується, бо система після отримання сигналу може перейти у будь який з двох атракторів. Якщо атракторам надається значимість у зв'язку з певною задачею, яку має вирішувати система, то прийнятим сигналам надається смисл, який залежить від цілей вирішення задачі. Залежно від прийнятого сигналу система буде знищувати, або зберігати, або створювати інформацію. Середню величину зміни інформації можна визначити як, так званий, її приріст за допомогою „інформації Кульбака":

$$K(p^{'}, p) = K\sum_{j} p_j^{'} \ln \frac{p_j^{'}}{p_j}, \qquad (6)$$

де $p_j$ – функція розподілу ймовірностей до прийому сигналу; $p^{'}_j$ – функція розподілу ймовірностей після прийому сигналу. З найбільшою ймовірністю реалізується та функція розподілу ймовірностей $p_i$, яка відповідає найбільшому числу можливостей і тим самим несе найбільшу інформацію.

З проведеного аналізу випливають такі проміжні висновки відносно відкритих систем. Фізична система, яка може обмінюватись із зовнішнім світом енергією та ентропією, називається відкритою. Знайдено, що багато відкритих фізичних систем виявляють властивість складних нелінійних структур і процесів –властивість самоорганізації. У процесах самоорганізації суттєву роль відіграє інформація (негентропія). Властивості самоорганізації виявлені і описані фізико-математичними методами на квантовому рівні на границі між мікросвітом і макросвітом (на мезо рівні), але проявляються і в процесах на рівнях макросвіту. Зокрема, самоорганізація властива біологічним системам, а також соціальним системам, де власне і створюються системи інформаційної безпеки. У класичній фізиці інформаційний зв'язок з'являється при взаємодії складних нелінійних систем із стохастичною поведінкою, коли малий зовнішній вплив може приводити до сильних змін траєкторії у фазовому просторі. Крім того, можна сформулювати твердження, що інформація може з'являтись на верхніх рівнях ієрархічних систем внаслідок процесів самоорганізації на стиках сусідніх ієрархічних рівнів. Далі спробуємо виявити вплив явища самоорганізації на процеси забезпечення інформаційної безпеки. Для цього звернемося до теорії систем по фон Берталанфі.

Слід відмітити, що у напрямку досліджень теорії систем по М. Месаровичу намітилась деякі обмеження. По перше, чим вище складність системи, тим більші проблеми із застосуванням строгих математичних методів внаслідок великої кількості рівнянь, змінних у описанні об'єктів усе більшого розміру. Теорема Геделя про неповноту стверджує, що не існує повної формальної теорії, де були б доказовими усі істині теореми арифметики. Згідно з цим законом, неминуче наступає такий момент, коли число подробиць складної системи починає рости «швидше трансфінітної послідовності». У тих випадках, де вдалось математично описати процеси самоорганізації, у теорії катастроф та інших, доводиться аналізувати моменти високих порядків – до четвертого і вище. З іншого боку, темпи досліджень не відповідають темпам розвитку сучасних технологій, особливо комп'ютерних і телекомунікаційних. Серед математичних теорій недостатньо розвинуті математичні методи оперування з ієрархічними об'єктами, конструкціями, поняттями, процесами. Вказані недоліки переборюється у теоріях систем по фон Берталанфі.

## III Класифікація та загальні властивості відкритих систем

У теоріях систем по фон Берталанфі суттєву роль відіграє ієрархічна класифікація систем. Класифікація систем є „проекцією" на певну систему координат і в принципі повинна розглядатись у топологічному (багатомірному) просторі. Далі пропонується удосконалена багатомірна класифікація систем, яка представляє собою суперпозицію шкали складності систем фон Берталанфі, класифікації К. Боулдінга систем за їх відношенням до інформації [16] та групи додаткових однокоординатних класифікацій за рівнем інтелектуальності системи, за характером обробки даних і знань, за типом мови описання, за типом і парадигмою управління (рис. 1). У рамках запропонованої системної класифікації розглянемо результати, що мають відношення до теорій цінності інформації та інформаційної безпеки.

Класифікація фон Берталанфі за шкалою складності систем виділяє три етапи наукового аналізу систем. На першому етапі розглядається «організована простота» (механіка), на другому – «безладна складність» (статистична фізика), на третьому - «організована складність». Системи організованої складності бувають двох типів: ті системи, які створені людиною, спроектовані і побудовані людьми й призначені для вирішення певних задач; ті системи, які існують у природі, створені у самій природі або, інакше кажучи, які виникли в результаті самоорганізації.

Класифікація систем К. Боулдінга є „проекцією" на координату упорядкування систем за рівнем сприймання, переробки й видачі ними інформації та інформаційних потоків. Важливість цієї класифікації полягає у якісній оцінці можливостей обробки інформації для кожного рівня та визначення ролі і цінності інформації. Запропоноване суміщення класифікацій характеризуються такими особливостями. Шкали складності систем фон Берталанфі і класифікацію К. Боулдінга можна розглядати як некорельовані. Група додаткових однокоординатних класифікацій, які тут розглядаються, навпаки, є сильно корельованими і залежними від основної класифікації К. Боулдінга. Можна стверджувати, що поява якоїсь нової характерної прикмети чи властивості на одному з рівнів основної класифікації, буде означати появу відповідних нових прикмет чи властивостей у кожній з групи однокоординатних класифікацій на тому ж

рівні.

Умовна порядкова шкала складності систем К. Боулдінга у скороченому вигляді виглядає так.

1. Рівень статичної структури. Описуються статичні взаємовідносини між елементами структури. Існування статичних систем не зумовлюється потоками інформації. Нової інформації не виникає. Ентропія постійна. Енергія не змінюється. Існує інформація про систему. Кількість інформації при вимірюванні аналогових параметрів статичної системи визначається за допомогою диференційної або $\varepsilon$-ентропії [17]:

$$H(x) = -\int_{-\infty}^{\infty} p(x)\log_{\varepsilon} p(x)dx\,, \tag{7}$$

де $p(x)$ – функція густини розподілу неперервної величини $x$; $\varepsilon$ – величина порогу розрізнювання вимірюваної величини, інакше – характеристика похибки вимірювань.

2. Рівень простої динамічної системи з наперед визначеними, обов'язковими рухами. Існування динамічних систем не зв'язано з переробкою потоків інформації. Прикладом такої системи може бути годинниковий механізм, система регулювання із зворотним зв'язком, канал передачі повідомлень. У системі організованої простоти кількість інформації визначається ентропією Р. Хартлі за допомогою комбінаторного підходу. В системах неорганізованої складності, при врахуванні статистичних властивостей, кількість інформації, що міститься у повідомленні і сигналі визначається їх ентропією по К. Шеннону, тобто зменшенням невизначеності при виборі. З точки зору цінності інформації в системі розрізняють корисний сигнал і шум або завади чи спотворення сигналів.


**Рисунок 1 – Суперпозиція класифікацій систем за шкалами складності**

На рівні динамічних систем інформація виникає не лише при врахуванні статистичних властивостей, а й внаслідок самоорганізації. За складністю процесів самоорганізації вділяють такі її типи: самоорганізація

у однорідних середовищах; у нестійких системах та у системах з дисипацією; у системах з появою ієрархічних структур [10]. Самоорганізація у однорідних середовищах і виникнення структур виглядає як виведення деяких колективних степенів свободи на рівень, далекий від теплового і які можуть описуватись як узагальнені макроскопічні параметри. У нестійких структурах всі траєкторії у фазовому просторі розбігаються. Великого значення набувають початкові дані для визначення області фазового простору, у яку попаде траєкторія. Чим більш точніші початкові дані, тим більше інформації про майбутню траєкторію. Тоді кількість інформації визначається кількістю знаків після коми і пропорційна величині $\ln(V/\Delta V)$, де $V$ – повний об'єм фазового простору, $\Delta V$ – доля об'єму фазового простору у початковому стані. Самоорганізація у системах з дисипацією та декількома областями притягування у фазовому просторі була розглянута вище. Кількість інформації, яку необхідно повідомити системі для переводу у будь-яку точку протягування іншого атрактора визначається як $\ln(V/\Delta V)$, де $\Delta V$ – об'єм протягування іншого атрактора.

Більш складний тип самоорганізації виникає, якщо розвивається ієрархія структур з появою і взаємодією вже нових структурних елементів. У складних фізичних системах можуть проявлятись тенденції до їх розшарування на інформаційну та динамічну підсистеми і виникають системи з інформаційною поведінкою. Інформаційну підсистему складають ті структурні елементи, які можуть сильно впливати на динаміку системи порівняно малими збуреннями, які називають сигналами. Інформаційна підсистема буває організована досить складно і може відкликатись не лише на інтенсивність сигналу а й на його форму, що слід сприймати як відгук на «смислову» частину сигналу. Такі системи проявляють адаптаційну здатність до енергетичних та інформаційних потоків не рівноважного зовнішнього світу. В системах, де з'являється управляючий параметр $a$, визначають кількість взаємної інформації $I(X:Y)$, використовуючи поняття умовної ентропії. Якщо $X$, $Y$ – випадкові залежні величини, то

$$S(X \mid Y) = -\sum_x \sum_y p(x,y) \log p(x \mid y), \tag{8}$$

де p(x,y) – ймовірність того, що величина X приймає значення x, а величина Y приймає значення y; p(x|y) – ймовірність того, що величина X приймає значення x, при умові, що величина Y приймає значення y. Кількість взаємної інформації X, Y один про одного становить величину:

$$I(X:Y) = \sum_x \sum_y p(x,y) \log p(x,y) - \sum_x \sum_y p(x,y) \log p(x)p(y) = S(X) - S(X \mid Y). \tag{9}$$

де $S(X|Y)$ – невизначеність ситуації $x$, яка залишилась після отримання про неї відомостей $y$.

Якщо управляючий параметр $a$ є характеристикою випадкової управляючої величини $Y$, то з (9) можна знайти кількість інформації про сукупність $X$ динамічної частини системи при заданому значенні управляючих параметрів $a$ управляючої частини системи.

3. Рівень кібернетичної системи або механізму управління, або іншими словами, системи з керованими циклами зворотного зв'язку. У системах цього рівня інформація передається і аналізується. Це найпростіший рівень, де інформаційні потоки та їх переробка можуть впливати на систему. До цього рівня слід віднести більшість сучасних (не інтелектуальних) інформаційних систем, які обробляють дані і які отримали характерну назву «млинів байтів». Кількість інформації визначається згідно з алгоритмічним підходом як ентропія А. Колмогорова (див. формулу (3) у [7]) і інтерпретується як мінімальна довжина максимально стиснутої програми Машини Тюрінга, яка дозволяє побудувати (описати) даний об'єкт. Машина Тюрінга, як математична модель, є елементарним аксіоматичним об'єктом у базовій системі аксіом теорії алгоритмів і теорії автоматів, які входять до інформаційної теорії систем. На третьому рівні починають проявлятись цілі застосування інформації і формується поняття кількості (корисної) інформації як міри доцільності управління, тобто ймовірності досягнення цілі при управлінні. А. Харкевич у 1960 році висунув постулат, згідно з яким цінність інформації 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.

3.1. Між третім і четвертим рівнем можна ввести ще один рівень – рівень вірусів. З точки зору інформаційної безпеки С. Расторгуєв поділяє віруси на біологічні і програмні. Програмні віруси відносяться до шкодоносних програм. Програма вважається шкодоносною (шкідливою), якщо вона: здатна знищити, блокувати, модифікувати або копіювати інформацію, порушувати роботу ЕОМ або інформаційної мережі; попередньо не попереджує користувача про характер своїх дій; попередньо не запитує у користувача згоди щодо реалізації свого призначення. У термінах інформаційної безпеки може бути застосована така міра кількості інформації, як логарифм числа кроків алгоритму чи кількості команд програми, яка вирішує задачу подолання (злому) системи захисту. Міра цінності інформації має

відображати ступінь корисності повідомлення для користувача і залежить від того, яка задача вирішується, яка інформація була до приходу повідомлення і як трактується повідомлення користувачем. Цінність інформації може враховуватись у функції штрафів, наприклад, при вирішенні задачі методом експериментальних 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 вирішного алгоритму. Невизначеність задачі знаходиться як логарифм математичного очікування числа спроб, необхідних для вирішення задачі (див. формулу (7) у [7]).

4. Рівень „відкритої системи", тобто над кібернетичної структури, яка має властивості само зберігання. Цей рівень, на якому живе починає відрізнятись від неживого, може бути названий рівнем „клітини". На цьому рівні починає зароджуватись власне відношення системи до вхідної інформації, рівень є проміжним між пасивною і активною реакцією на вхідну інформацію.

5. Рівень „рослини", або, можна так назвати, „генетично-суспільний" рівень. Мова йде про специфічну форму реакції на збурюючу інформацію, притаманну рослинам, зокрема з пристосуванням та іншими реакціями на впливи.

6. Рівень „тварини", який характеризується наявністю рухливості, цілеспрямованою поведінкою і обізнаністю. Сприймаються значно більший потік вхідної інформації за допомогою спеціалізованих приймачів: очі, вуха, тощо. Є розвинуті нервові системи, які приводять до появи мозку. Мозок формує з вхідної інформації основні риси явища, або „образ". Поведінка не є простою відповіддю на якийсь вплив, а визначається „образом" або структурою знання про оточуючу обстановку в цілому. Між впливом і реакцією на цей вплив з'являється процес аналізу образу.

7. Рівень „людини". Окрема людина розглядається як система. Крім характеристик „тваринних" систем людина володіє самосвідомістю, яке відрізняє його від простої обізнаності тварини. Людська уява складніша, ніж у вищих тварин. Людина вже знає, що вона знає. Використовується мова та символи. Мова контекстно залежна у більшій мірі, ніж у тварин.

8. Рівень суспільного (соціального) інституту. Сюди відносяться системи, які організують науково-виробничу та громадську діяльність. Їм притаманні тонкий символізм мистецтва, музики та поезії, складна гамма людських емоцій.

9. Завершують ієрархію систем – трансцендентні системи. Існування такого більш складного класу систем можливе у випадку, якщо правомочне твердження про можливість повного відриву інформації від фізичного носія.

У ієрархії систем рівні, які складніші ніж третій «кібернетичний» рівень, виділяються під загальною назвою «надкібернентичні», або, як прийнято у роботах фон Берталанфі, К. Боулдінга, Дж. Міллера та інших вчених, «живі системи». Надкібернетична система – це система, рівень складності якої не дозволяє створити модель, адекватну множині можливих цілей дослідження, на рівні системи зі зворотними зв'язками. Для таких систем сьогодні неможливе знаходження їх строгого класичного математичного описання. У розглянутій класифікації нема поділу аналогічного ряду: мікросвіт-макросвіт-всесвіт. Ієрархія у даній класифікації розглядається лише за складністю інформаційних процесів у системах. Принциповим є те, що надкібернетична система може існувати лише як відкрита система. Значну роль відіграють властивості самоорганізації та самозберігання, а також динамічні властивості інформаційних процесів. Кількість інформації можна визначати мірою А. Колмогорова, а приріст інформації при самоорганізації визначається інформацією Кульбака (6). Цінність інформації визначається ймовірністю досягнення цілі при управлінні, тобто мірою А. Харкевича.

Теорія інформації відкритих систем продовжує розвиватись в інформодинаміці. Інформодинаміка – це наука про інформацію як про явище, її структуроутворення, фундаментальні властивості інформації як управління для системно-складних об'єктів та управляючої сутності інформації у її взаємодії з об'єктами управління. Методи інформодинаміки поки що не спираються на певний математичний апарат. Її поняття і побудова формуються за допомогою логічних конструкцій, а точніше методом динамічного моделювання з елементами самокорекції. Основами інформодинаміки є теорія інтелектуальних систем управління та теорія структурної узгодженості як технологія конструювання відкритих систем. Слід відмітити, що сучасні складні інформаційно-комунікаційні мережі розвиваються дещо схожим способом. Спочатку вони будувались на солідній математичні базі – теорії телетрафіку, розробленої датським математиком А. Ерлангом, теорії масового обслуговування, ланцюгів Маркова, теорії графів тощо. Нині розвиток комп'ютерних мереж, Інтернет, телекомунікаційних та інформаційних технологій, нових протоколів, інтерфейсів відбувається без помітного розвитку відповідних прикладних математичних теорій, за винятком кібернетичних. Серед математичних методів дослідження переважним є імітаційне моделювання. Часом самі мережі та її елементи в процесі свого розвитку стають полігоном для оцінки,

відбору, самокорекції і вдосконалення.

В запропонованій класифікації існуючі системи інформаційної безпеки займають декілька рівнів. За своїм призначенням і цілями вони створюються у середовищі рівня соціальної системи. Об'єктами інформаційної діяльності можуть бути фізичні динамічні і кібернетичні системи, системи технологічного чи суспільного управління. Будучи комплексною системою організаційних, організаційно-технічних та технічних засобів системи інформаційної безпеки мають риси ергатичних – людино-машинних систем. Організаційні заходи відносяться до рівня людини і соціальної системи, технічні засоби – відносяться до рівня фізичних динамічних систем, а програмно-технічні засоби – реалізуються кібернетичними системами. Тому в ієрархічній класифікації систем слід враховувати вертикальні зв'язки між рівнями: знизу наверх і зверху до низу. З переходом від нижчих рівнів до вищих у ієрархічних системах діють закони утворення нових об'єктів та інтегральних параметрів, подібних до макроскопічних. На квантовому рівні існують квантові мікрочастки з їх ансамблями станів, термодинамічними процесами дисипації з ростом ентропії та зворотними нелінійними процесами самоорганізації зі зменшенням ентропії за рахунок росту ентропії оточення. На макрорівні з'являються макроскопічні параметри порядку: температура, щільність, тиск тощо. У напрямі зверху вниз у ієрархії систем нас цікавлять впливи верхніх рівнів на інформаційну безпеку систем нижніх рівнів та методи побудови інформаційно безпечних систем, що взаємодіють в процесах інформаційного управління. Перейдемо до аналізу структурних властивостей інформації, включаючи інтелект і появу розуму.

## IV Структурні властивості інформації та інформаційних процесів у відкритих системах

В ієрархії систем з ростом рівня стрибкоподібно якісно змінюється смисл сприймання і обробки інформації, відбувається перехід від сигнального і контекстно-вільного до структурного та контекстно-залежного аналізу інформації. Значимість інформації підвищується в міру зростання організаційної і поведінкової складності систем. Змінюється форми представлення, описання, моделювання та структура інформації. З ростом рівня представлення інформації ускладнюється від даних до знання та інтелекту. При цьому управляюча сутність інформації стає все більш значимою.

Дані і знання – це структуроутворюючі поняття [5]. *Дані* складаються з опису об'єктів, їх оточення, явищ, фактів. Описи реалізуються на мовах, доступних для сприймання та інтерпретації суб'єктами. *Знання*, в загальному випадку, є: змінною у часі і контексті сукупністю іменованих відносин між даними та представленими, для використання інформації, мовою, здатною нести і передавати дані і знання про предметну область; рівно зрозумілими (тобто такими що сприймаються у одному контексті) двом і більше системам, які спілкуються на рівні знання; достатніми, у сукупності з даними, для інформаційного забезпечення вирішення деякої задачі або сукупності задач інтелектуальної системи. Можна виділити декілька рівнів представлення знання у його зв'язку з даними та мовами, якими можливо представлення інформації як управління: рівень фактографічної моделі, рівень математичної моделі, рівень інформаційної системи та рівень інтелектуальної системи. На рис. 1 група цих класифікацій зіставляється з класифікацією К. Боулдинга.

На рівні фактографічної моделі використовують текстові записи з фіксованою на рівні мови їх представлення системою відношень між ними, наприклад, табличні записи. На рівні математичної моделі дані формалізуються на рівні мови формул і передаточних функцій, містять у собі знання як формалізовані правила та апарат проведення виведень. Використовується функціональна мова математики, мови описання функціональних зв'язків, які використовують математичні символи, існуючі і спеціально розроблювані математичні функції, різного роду математичні вирази, які економно описують дані та їх взаємозв'язки. Взаємозв'язки – жорсткі, взаємодія з оточенням – лише в межах передбачених зв'язків. Математичні мови базуються на певних наборах початкових посилок і угод, аксіоматика яких є окремим предметом математики і завжди зв'язана з геделівською теоремою про неповноту. В межах вибраної моделі вони є абсолютним апаратом вироблення правильних рішень і гарантовано точно описують процеси управління при виконанні угод про модель. Всі сигнали і пристрої адекватно задачі описуються обраною математичною мовою. Але доказового вибору моделі практично не існує. Вибір моделі завжди є мистецтвом і правильність вибору моделі перевіряється практикою.

На рівні інформаційної системи знання і дані існують у формі мовної моделі, яка виділяє із реальної системи дещо визнане «істотним». Модель описується за допомогою контекстно-незалежних алгоритмічних мов. Знання розуміється як процедура єдино можливої інтерпретації зв'язків даних. Відношення між даними незмінні і визначені початковою структурою бази даних. Можна сказати, що це рівень фіксованого знання, довідкових відомостей, доповнених можливістю актуалізації даних, але не зв'язків між ними. З точки зору інформаційної безпеки, будь-які завчасно не передбачені відхилення

теоретичного описання об'єкта від його практичного стану можуть вести до катастрофічних наслідків. Наприклад, у системах технічного захисту інформації основною задачею є виявлення технічних каналів витоку інформації та їх блокування.

Контекстно незалежні алгоритмічні мови базуються на певному наборі попередньо введених домовленостей – команд і дій комп'ютера при їх виконанні. Функціональна повнота та вимоги несуперечності цих мов є менш строгою, ніж математичних мов. Алгоритмічні мови описуються домовленостями, заданими на метамові, що дозволяє гарантувати однозначність розуміння допустимих термінів і команд у всіх можливих ситуаціях. Мови такого роду називають мовами програмування. Вони застосовуються тоді, коли ці дії не можуть бути задані більш економним, математичним представленням або враховують деякі часткові характеристики сигналів чи обладнання, або забезпечують більш ефективне описання, ніж математичні мови (наприклад спискові структури). Але всі взаємозв'язки, характеристики пристроїв, можливі ситуаційні і часові умови мають бути передбачені завчасно. Тут гарантується вироблення доцільних рішень на основі застосування евристичного апарату вироблення доцільних рішень. Мови такого типу корисні та придатні для кібернетичного рівня моделювання системно-складних об'єктів. Але доказового вибору моделі тут також не існує. Кількість можливих станів реальної інформаційної системи може бути більшим, ніж кількість станів моделі, яка її описує. З точки зору інформаційної безпеки будь-які завчасно не передбачені відхилення практичного стану об'єкта від його теоретичного описання (тобто вразливості автоматизованої системи) повинні бути заблоковані у процесі створення системи захисту, щоб вони не могли вести до катастрофічних наслідків. Виникає практично не вирішувана проблема «змагання» між процесами пошуку вразливостей і процесами їх усунення.

На рівні інтелектуальної системи знання і дані існують у формі мовної моделі предметної області і як описання складових цієї системи на рівні контекстно-залежної мови. Такі моделі, у багатьох, якщо не в усіх, випадках невідрізнимі від самої предметної області, існуючої як мова описання. Знання зв'язане з вираженням контекстно-залежних відношень між даними. Тут знання виражається поточною структурою зв'язків між даними у деякій інформаційній базі, яка змінюється після кожного акту спілкування, після обробки кожного вхідного повідомлення на контекстно-залежній мові. Це вища інженерна форма представлення знань, яка допускає для збереження семантики інтерпретації даних як актуалізацію цих даних і можливих типів відношень між ними, так і актуалізацію самої структури їх зв'язків у процесі суб'єкт – управляюча дія – об'єкт. Контекстно-залежні мови можуть бути використані як командні повідомлення для систем управління, які існують (спостерігаються) на основі цих мов і які здатні сприймати такі команди. Базування на автоматах будь-якого виду веде до спрощення КЗ мови, збідненню його синтаксису і семантики з метою забезпечення однозначного незмінного розуміння. Приклади: ієрархічна класифікація, мови з фіксованими відношеннями, проблемно-орієнтовані мови, наближені до природних тощо. При реалізації необхідне зберігання даних, яке зберігає синтаксис, семантику і прагматику КЗ мови, тобто зберігання знань на рівні можливості розуміння контексту, забезпечити орієнтацію системи управління на різні контексти інформаційних потоків у різних ситуаціях тощо. Ставиться задача (інтелектуальності) управління на семантично зв'язаних потоках інформації.

Х. Рамперсад вважає, що знання – це функція від інформації, культури і навиків. *Знання = f* (*інформація; культура; навики*) [17]. Під терміном інформація у даному контексті розуміється значення, яке надається даним відповідно до певних запитів чи потреб. Такі дані носять також назву «явних знань». Явні знання не залежать від індивіду. Воно є теоретичним від природи і засноване на алгоритмах, теоріях, системах рівнянь, методичних керівництвах, схемах та інших джерелах. Цей вид знань закладають у системи управлінської інформації, у технічні системи, у організаційні процеси. Компоненти знання, які характеризують культуру і навики, являють собою «неявні знання». Культура є сукупністю норм, цінностей, поглядів принципів і відношень людей, яка керує їх поведінкою та діями. Навики зв'язані зі здібностями, уміннями людей та індивідуальним досвідом. Неявні знання залежать від конкретної людини і зберігаються в її пам'яті. Вони є практичними за природою зі знаходять джерела свого поповнення, серед іншого, в інтуїції. Знання ведуть до компетентних дій. Але знання старіють дуже швидко і легко втрачають свою актуальність. Саме тому вчитись необхідно постійно.

З точки зору окреслення майбутніх вимог до інформаційної безпеки відкритих систем важливо сформулювати поняття «навчання». В даному випадку навчання – це неперервна трансформація особистості, це циклічний і кумулятивний процес актуалізації знань, тобто додавання нової інформації до вже існуючої з метою змінити поведінку таким чином, щоб можна було діяти більш ефективно.

Дані не існують без відносин між ними (того чи іншого варіанту впорядкованості, яка змінюється у ту чи іншу сторону в міру отримання нових інформаційних посилок. У знаннях дані не відрізняються, а нерозділимі зі знанням і поточним контекстом інтерпретації. Коли знання перестає бути процесом, а контекст наперед визначений – інтелект зникає. З даними і знаннями, представленими мовними моделями,

доцільно працювати у предметних областях з переважанням емпіричного знання, де складність фактів та їх описання виключає використання мови математики – це так звані описові науки, які вивчають те, що не може бути адекватно забезпечено мовою математики – відкриті системи у їх природному оточенні.

Сукупність знання-дані в задачах управління представляється деякою семіотичною системою. Семіотика – це наука про знаки та знакові системи. У семіотичній системі зазвичай виділяють три аспекти: синтаксичний, семантичний і прагматичний. Необхідно виділити три типи знань як три типи відносин між даними: синтактичні, семантичні і прагматичні.

Знання синтаксичного типу характеризують синтаксичну структуру потоку інформації, яка не залежить від смислу і змісту використовуваних при цьому понять, тобто інтелектуальну систему не утворює. Саме тут доцільне застосування понять кількості інформації (кількості синтаксичної інформації) – по Хартлі, Шенону і Колмогорову. Семантичне знання розглядається як структура, яка утворює поточний контекст. Воно містить інформацію, безпосередньо зв'язану з поточними даними смислом описуваних понять і наперед визначає стан знаків даних у інформаційній базі. Тут ми маємо справу з певною структурою і ця структура повинна складатись із певного (функціонально повного) набору деяких елементів. В. Лачинов та А. Поляков запропонували такі елементи, які названі інфокварками [5] і слугують «будівельними» елементвми інфомодинамічних комп'ютерів. За допомогою них можна вимірювати «семантичну» кількість інформації.

Прагматичне знання наперед визначає найбільш ймовірні зв'язки, які описують дані з точки зору вирішуваної задачі (узагальнений або «об'єктивний» контекст), наприклад з урахуванням діючих в даній задачі специфічних критеріїв і домовленостей сфери інформаційної безпеки. Поняття об'єктивності відповідає трактовці прагматики створення інтелектуальної системи як направленого обмеження її «свободи», обмеження непотрібних зв'язків і «фантазії зв'язків за контекстами». З інженерної точки зору, синтаксична, семантична і прагматична сторони знання є різними зв'язками одного або групи термінів (даних) з іншими записами у інформаційні базі.

Із сказаного ясно, що найбільш загальна проблема побудови системи управління (з урахуванням інформаційної безпеки) семантичного або семантико-прагматичного рівня зв'язана з вибором технології контекстно-залежного представлення знань, побудови інформаційних баз про предметну область (в тому числі даних і знань бази захисту) та механізму виводу для одержання необхідних рішень.

Як проміжний висновок дамо робоче визначення відкритої системи, яке застосовано у прикладній теорії інтелектуальних систем управління і яке будемо використовувати у другій частині даної роботи. Під відкритою (інтелектуальною, що тотожно) системою розуміється сукупність активних суб'єктів і об'єктів (суб'єктів), які їм протистоять, породжувана або ситуаційною можливістю (свободою волі) активного існування об'єкта, або цільовою задачею (непереборним зовнішнім впливом на свободу волі) деякого системного або позасистемного суб'єкта, причому всі елементи любої природи, які складають відкриту інтелектуальну систему, знаходяться під впливом зовнішнього світу.

Вивчаючи відкриті системи, ми переходимо від функціональних моделей систем, заданих мовою передаточних функцій, до реальних систем у їх зовнішньому оточенні, доступних нам без втрат лише мовою, рівень складності якої забезпечує їх понятійну взаємодію із «зовнішнім керівним суб'єктом» і ідентифікацію семантики їх взаємодії із зовнішнім світом. Усі складні системи, як і інтелект, існують лише як процес. Ізоляція від зовнішніх взаємодій приводить до деградації відкритої системи.

**Результати та проміжні висновки.** Зроблена спроба проаналізувати вплив останніх досягнень інформаційних технологій на вирішення проблем інформаційної безпеки. Уточнено поняття інформації як об'єкта захисту й цінності інформації. Напрям подальшої роботи – дослідження властивостей моделей цінності інформації та застосування їх при проектуванні систем інформаційної безпеки телекомунікацій.

*Література: **1.** Закон України «Про основи національної безпеки України» від 19.06.02, №964. **2.** Закон України „Про телекомунікації" від 18.11.2003, № 1280. **3.** НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Введ. 01. 07. 99. – К.: ДСТСЗІ СБ України, 1999. – 26 с. **4.** Килин С. Я. Квантовая информация. // Успехи физических наук, Том. 169, № 5, Май 1999. – С. 509 – 527. **5.** В. М. Лачинов, А. О. Поляков. Информодинамика или Путь к Миру открытых систем. Санкт-Петербург, Издат. СПбГТУ, 1999. – С. 364. (http//www.polyakov.com/informodynamiks). **6.** Широчкин В. П. Архитектоника мышления и нейроинтеллект. /Под ред Ю. С. Ковтанюка – К.: Издательство Юниор, 2004. – 560 с. 7 Кононович В. Г., Тардаскін М., Тардаскіна Т. Моделі цінності інформації з позицій інформаційної безпеки інформаційно-телекомунікаційних систем. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, К: 2004. С 30 – 39. **8.** Месарович М., Такахара Я. Общая теория систем: Математические основы. М.: Мир, 1978. **9** .*

*Берталанфи Л. фон. Общая теория систем: Критический обзор // Исследования по общей теории систем. М.: Прогресс, 1969 с. 23-82.* ***10.*** *Кадомцев Б. Б. Динамика и самоорганизация. УФН. 164, №5, 4491994) – 396 с. 11. Бриллюен Л. Наука и теория информации. М.: Физматгиз, 1960.* ***12.*** *Кулик С. П. Физические основы квантовой информации. Лекции физ. фак. МГУ. http://qopt.phys.msu.su/speckurs/quantinf/lecture.pdf.* ***13.*** *Манойло С., Оскома Р. Квантовые вычисления. Алгоритмы эффективного решения NP-полных задач. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 11, К: 2005. С 153 - 157.* ***14.*** *Блюменфельд Л. А. Информация, термодинамика и конструкция биологических систем. // Соросовский образовательный журнал, № 7, 1996. – С. 88 – 92.* ***15.*** *Хакен Г. Информация и самоорганизация: Макроскопический подход к сложным системам: Пер. с англ.–М.: Мир, 1991. – 240 с.* ***16.*** *Боулдинг К. Общая теория систем - скелет науки // Исследования по общей теории систем. М.: Прогресс, 1969 с. 106-124.* ***17.*** *Стратонович Р . Л. Теория информации. – М.: Сов. Радио. 1975. – 424 с.* ***18.*** *Рамперсад К. Хьюберт. Универсальная система показателей деятельности: Как достигать результатов, сохраняя целостность / Пер. с англ. – М.: Альпина Бизнес Букс, 2005. – 352 с.*

**УДК 681.321;322:621.395**

# ПАРАДИГМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕБІОМЕТРИКИ ТА СЕНСОРНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

***Володимир Кононович, Микола Тардаскін****

*Академія зв'язку України, *Одеський регіональний центр ТЗІ ВАТ "Укртелеком"*

*Анотація:* **Аналізуються аспекти захищеності та інформаційної безпеки телебіометрики і бездротових сенсорних мереж при взаємодії людей між собою та навколишнім середовищем з використанням моделі, рекомендованої міжнародним стандартом МСЕ-Т (Рекомендація Х.1081). Розглядається парадигма інформаційної безпеки нових інформаційних технологій.**

*Summary:* **Aspects of security both information safety of the telebiometric and Wireless Sensor Networks are analyzed at interaction of people among themselves and by an environment with use of the model recommended international standard (ITU-T Recommendation X.1081). The paradigm of information security of new information technologies is considered.**

*Ключові слова:* **Інформаційна безпека, захищеність, телекомунікаційні мережі, сенсорні мережі, телебіометрика, особиста сфера приватності, парадигма інформаційної безпеки.**

## І Вступ

Розвинуте і стабільне інформаційне суспільство характеризується можливістю та спроможністю держави створювати умови для вільного доступу своїх громадян до інформаційних ресурсів, та умінням захищати національні інформаційні ресурси, інтереси особи, суспільства та держави в цілому від внутрішнього і зовнішнього негативного впливу [1]. При цьому, у сфері захисту інформаційних ресурсів необхідно забезпечувати надійне, безпечне функціонування національної інформаційної інфраструктури та її подальший ефективний розвиток. Існуюча парадигма класичного технічного захисту інформації полягає в забезпеченні збереження заданих властивостей інформації та інформаційно-телекомунікаційної системи, а саме: конфіденційності й цілісності інформації, доступності ресурсу системи, цілісності і спостережності інформаційно-телекомунікаційної системи [2]. Класична система технічного захисту інформації заснована, головним чином, на автономності і локальності інформаційних ресурсів інформаційної системи. Концепція захисту передбачала, як головні задачі, обмеження кола користувачів і створення системи розмежування доступу користувачів до інформації за категоріями.

З розширенням сфери застосування інформаційних технологій, глобальним розповсюдженням Інтернет, активним впровадженням доступу до розподілених баз даних за технологією клієнт - сервер з'являються операційні системи з багаторівневим захистом від несанкціонованого доступу, застосовується криптографія для шифрування транзакцій, впроваджуються засоби блокування підключення пристроїв. Має розповсюдження концептуальна технічна модель ешелонованої багаторівневої системи інформаційної безпеки міжнародного стандарту ISO/IEC 15408 [3], який визначає нову технологію розробки профілів захисту та проектів безпеки. Ряд фахівців пропонують впровадити цей стандарт в Україні [4], такий стандарт вже введений в Російській Федерації методом "обкладинки" [5]. Концептуальна модель системи інформаційної безпеки включає в себе набір послуг безпеки (та механізмів безпеки, які ці послуги реалізують), що забезпечують функції моніторингу, захисту та застосування інформаційних ресурсів з