001-2000. Типове положення про службу захисту інформації в автоматизованій системі. ДСТСЗІ СБУ, 2000; ***8.*** *НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 2000;* ***9.*** *НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 2001;* ***10.*** *НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. ДСТСЗІ СБУ, 2002;* ***11.*** *НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. ДСТСЗІ СБУ, 2003;* ***12.*** *НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.* ***13.*** *НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;* ***14.*** *ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;* ***15.*** *ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;* ***16.*** *ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.*

УДК 004.056: 004.942

СИСТЕМНИЙ ПІДХІД У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Віталій Носов

Харківський національний університет внутрішніх справ, м. Харків

Анотація: **Запропоновано використання системного підходу в забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем. Представлена формальна модель і ключові характеристики мережі взаємин комплексної системи захисту інформації в складі узагальненої інформаційно-телекомунікаційної системи.**

Summary: **Approach Systems to information security of corporate information and telecommunication systems is proposed. The formal model and key characteristics of network relationships Information Security Complex System consisting in a Common Information and Telecommunication System is represented.**

Ключові слова: **Системний підхід, інформаційна безпека, формальна модель.**

I Вступ

Для забезпечення інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем створюються і експлуатуються системи захисту інформації, які, як і інші створені людиною організаційно-технічні системи, в своїй більшості мають суттєві недоліки, а саме:

- створені, як правило, без належного обґрунтування затрат;
- експлуатуються без оцінювання ефективності роботи;
- технічно реалізовані, але не використовуються;
- розроблені на стадії технічного проекту, але не впроваджені в діючу інформаційно-телекомунікаційну систему;
- і таке інше.

Одним із шляхів концептуального подолання більшості відомих вад систем захисту інформації є створення *життєздатної* системи захисту інформації, що потребує, на думку автора, системного мислення та системного підходу.

Метою статті є:

- представлення математичної моделі системи захисту інформації у складі корпоративної інформаційно-телекомунікаційної системи;
- формулювання ключових характеристик системного мислення та системного підходу у забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем.

II Основна частина

Системне мислення та системний підхід

Що таке система? За визначенням основоположника загальної теорії систем Ludwig von Bertalanffy [1] система – це сукупність елементів, що знаходяться в певних стосунках один з одним і з середовищем. Або за

іншим визначенням, система – це впорядкована певним чином множина елементів, які пов’язані між собою і утворюють цілісну єдність [2].

В основі системного мислення лежать поняття зв'язності, взаємин і контексту[1]. Згідно з системним мисленням істотними властивостями системи (живої або неживої), є властивості цілого, якими не володіє жодна з його частин. Нові властивості виникають із взаємодій і взаємин між частинами. Ці властивості порушуються, коли система фізично або теоретично розтинається на ізольовані елементи. Хоча можна розпізнати індивідуальні частини в будь-якій системі, але ці частини не ізольовані, і природа цілого завжди відрізняється від простої суми його частин.

Систему не можна пізнати за допомогою аналізу. Властивості частин не є їх внутрішніми властивостями, але можуть бути осмислені лише в контексті крупнішого цілого. При системному підході властивості частин можуть бути виведені лише з організації цілого. Системне мислення не концентрує увагу на основній «цеглі», а досліджує основні принципи організації. Системне мислення контекстуально і є протилежним аналітичному мисленню. Аналіз означає відділення чого-небудь, з тим аби зрозуміти його, а системне мислення означає переміщення чого-небудь в більш широкий контекст цілого.

Ключові характеристики системного мислення та системного підходу полягають у наступному [3].

Перехід мислення від частин до цілого. Системи є інтегрованими цілісностями, чиї властивості не можуть бути зведені до властивостей їх дрібніших частин. Їх істотні або системні властивості - це властивості цілого, якими не володіє жодна з частин. Нові властивості з'являються з організуючих стосунків між частинами, тобто з конфігурації впорядкованих взаємин, характерної для конкретного класу систем. Системні властивості порушуються, коли система розтинається на ізольовані елементи.

Переміщення фокусу уваги з одного рівня системи на інший. В межах живого світу ми знаходимо системи, включені в інші системи, і, застосовуючи одні і ті ж поняття до різних системних рівнів, пізнаємо їх. З іншого боку різні системні рівні відрізняються рівнями складності. На кожному рівні спостережувані явища відрізняються властивостями, яких немає на нижчих рівнях.

Пояснення речей в термінах зовнішнього середовища.

Перехід від пізнання об'єктів до пізнання взаємин між об’єктами. Мислячи системно, потрібно розглядати **об'єкти як мережі взаємин**, які включені в більш широкі мережі (рис. 1). Первинними є взаємини, а кордони помітних об'єктів (паттернів[2]) вторинні, як це спрощено показано на рис. 1.

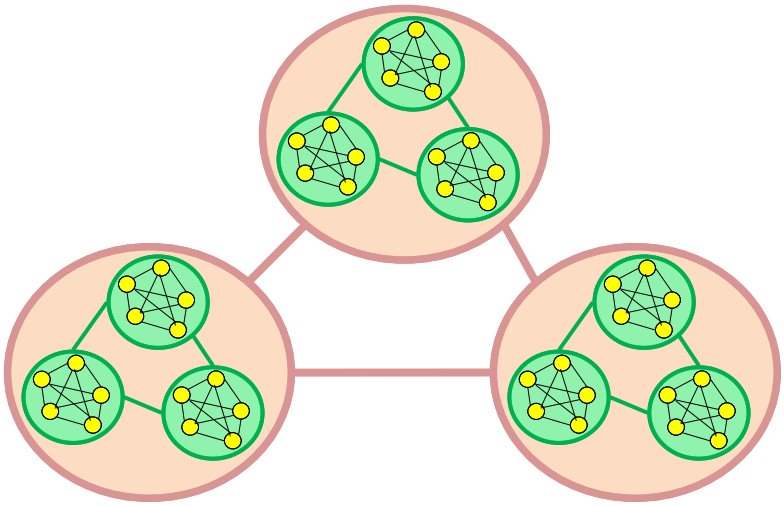

Рисунок 1 – Мережі взаємин

Уявлення про наукове знання як про мережу понять і моделей, в якій ні одна частина не більш фундаментальна, ніж інша. Ця парадигма була сформульована в 1960-і роки фізиком Geoffrey F. Chew у вигляді так званої Bootstrap-теорії [4, 5]. Філософія Bootstrap-теорії не тільки відкидає ідею фундаментальних цеглинок матерії, але взагалі не приймає ніяких фундаментальних сутностей – ні фундаментальних констант, ні фундаментальних законів або рівнянь. Матеріальний всесвіт розглядається як динамічна павутина взаємопов'язаних подій. Ні одна властивість будь-якої частини цього павутиння не є фундаментальною, і всі

[1] **Контекст** (лат. contextus – тісний зв’язок, сплетення) – середовище, в якому існує об'єкт.
[2] **Паттерн** *(*англ. pattern – зразок, приклад, принцип*)* – конфігурація впорядкованих взаємин.

вони випливають з властивостей інших частин, і загальна узгодженість їх взаємозв'язків визначає структуру всього павутиння.

Епістемологія[3] *(опис процесу пізнання) має бути явним чином включена в опис досліджуваних феноменів.* Спостерігач завжди є учасником досліджуваного процесу. Для того, щоб у взаємозв'язаному павутинні елементів реального світу виділити для вивчення якийсь об'єкт, спостерігач обриває деякі зв'язки вибраного паттерну з рештою світу – як концептуально, так і фізично за допомогою приладів для спостереження, – і, діючи таким чином, ізолює деякі паттерни та інтерпретує їх як об'єкти. Обрив зв'язків викликає трансформацію властивостей даного паттерну. З цього випливає наступна характеристика системного підходу.

Всі наукові поняття і теорії обмежені та приблизні. Опис явищ може бути лише приблизним (із зазначенням умов дослідження). Усі явища в нескінченній множині в природи взаємозв'язані, тому, аби дати повне пояснення хоч би одному з них, спостерігач має знати і розуміти всі інші, що вочевидь неможливо.

Системне мислення та системний підхід для систем захисту інформації

Система захисту інформації є частиною інформаційно-телекомунікаційної системи. Інформаційною системою, найвищою за рівнем узагальнення і складності, можна вважати Людину (Homo sapiens, HS), яка своєю розумовою діяльністю створює, оброблює, зберігає, приймає, передає інформацію в інші системи, наприклад в інформаційно-телекомунікаційну систему (information and telecommunication system, ITS). Нижче HS за рівнем узагальнення і складності можна вважати ITS у вигляді структурованих *продуктів,* між якими існують взаємини (*процеси*). Таким чином, ієрархію за рівнем узагальнення і складності об’єктів *узагальненої інформаційно-телекомунікаційної системи* (Common ITS, CITS) можна представити орієнтованим графом (рис. 2):

$$\mathrm{G}_{\mathrm{CITS}}(\mathrm{V},\mathrm{E}) = \{\{\mathrm{product}, process, ITS, HS\}, \{\langle \mathrm{product}, ITS\rangle, \langle process, ITS\rangle, \langle ITS, HS\rangle\}\}. \quad (1)$$

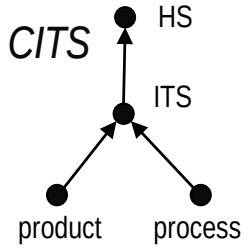

Рисунок 2 – Орієнтований граф ієрархії за рівнем узагальнення і складності об’єктів узагальненої інформаційно-телекомунікаційної системи (Common ITS, CITS) $G_{CITS}(V, E)$

Кожна штучно створена система має життєвий цикл – від створення до закінчення існування. Життєвий цикл створеної системи (System Development Life Cycle, SDLC) можна поділити на фази, як це запропоновано, наприклад, в [6].

1. *Ініціювання (Initiation).* Описується цільове призначення та функції створюваної системи.
2. *Створення (Development/Acquisition).* Проектування та виготовлення системи.
3. *Оцінка/Впровадження (Implementation/Assessment).* Оцінка якості та подальше впровадження створеної системи в експлуатацію.
4. *Експлуатація (Operation/Maintenance).* Використання системи за призначенням, в подальшому її модифікація.
5. *Видалення (Disposal).* Коректне завершення існування системи, перенесення необхідної інформації в нові системи.

Інформаційну безпеку CITS представимо як перебування CITS в бажаних для людини (власника інформації або CITS) станах. При цьому "бажані стани" природно змінюються при зміні відповідних потреб людини (власника інформації або CITS). Забезпечити перебування CITS в "бажаних станах" може наявність у складі CITS деякої підсистеми, а саме – *комплексної системи захисту інформації* (Information Security Complex System, ISCS). ISCS – це складова частина CITS із специфічними функціями, яку неможливо відокремити від CITS, тому далі будемо оперувати зв’язкою CITS-ISCS. Ієрархію за рівнем узагальнення і складності об’єктів систем CITS-ISCS з урахуванням фаз SDLC можна представити як на рис. 3.

[3] **Епістемологія** (грец. επιστήμη – знання, λόγος – вчення) – теорія пізнання.

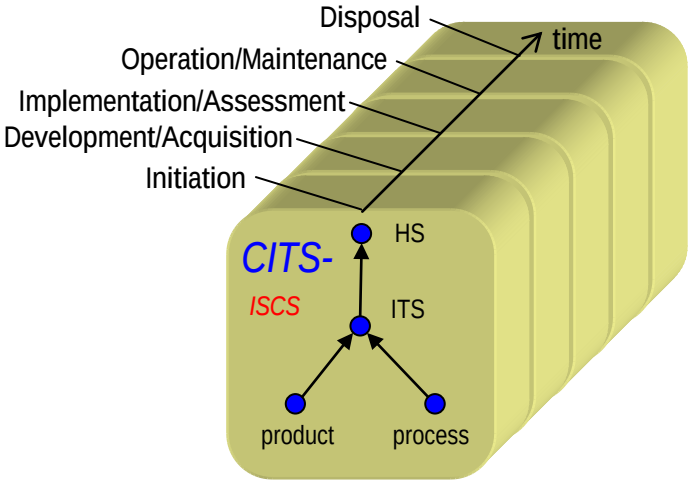

Рисунок 3 – Фази життєвого циклу систем CITS-ISCS

Представимо системи CITS-ISCS через мережу взаємин (процесів) між структурованими продуктами (складовими ITS) та користувачами (HS) (рис. 4). Відмітимо, що процеси (взаємини) можуть існувати між системами різного рівня складності.

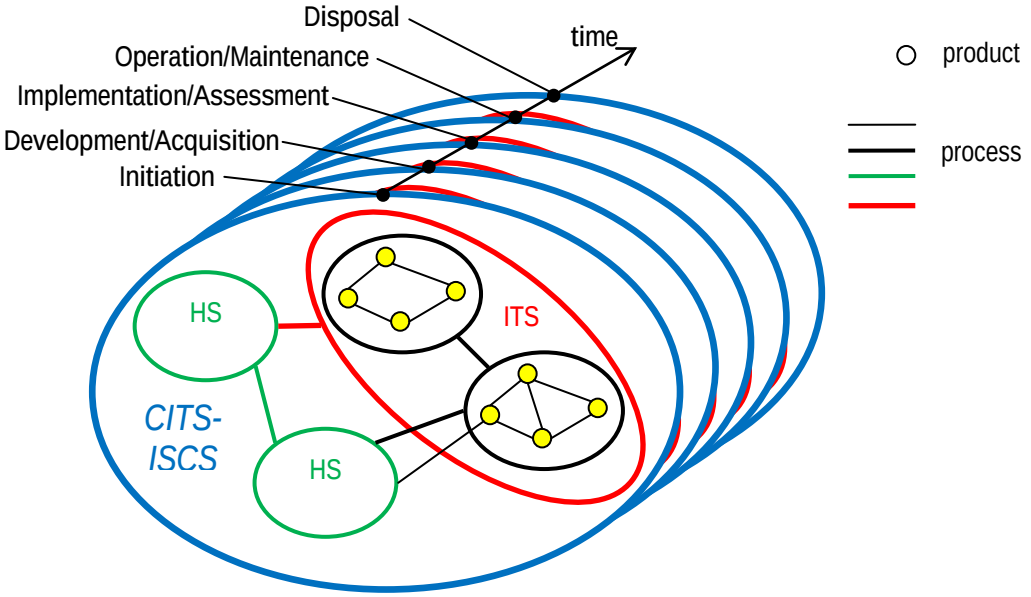

Рисунок 4 – Модель мережі взаємин CITS-ISCS

Модель мережі взаємин CITS-ISCS представимо формально *п'ятифазовим* (за фазами SDLC) *гіперграфом*

$$H_k^0(X_k^0, U_k^0),\ k \in K = \{1,2,3,4,5\},\quad X_k^0 = \{x_{k1}^0, x_{k2}^0, \ldots, x_{km}^0\},\ U_k^0 = \{u_{k1}^0, u_{k2}^0, \ldots, u_{kn}^0\}, \qquad (2)$$

де X_k^0 - множина вершин (об'єктів найнижчого рівня складності і узагальнення CITS-ISCS), U_k^0 - множина ребер, кожне з яких є підмножиною двох і більше вершин $u_{kj}^0 \subseteq X_k^0$ (рис. 5).

З гіперграфу $H_k^0(X_k^0, U_k^0)$ можна отримати частину гіперграфу $H_k^1(X_k^1, U_k^1)$, який буде відображати системи з більшим рівнем складності і узагальнення. Визначення вершин і ребер гіперграфу $H_k^1(X_k^1, U_k^1)$ через елементи $H_k^0(X_k^0, U_k^0)$ можна здійснити такими функціями:

$f : U_k^0 \to X_k^1$ - вершини гіперграфу більш високого рівня складності і узагальнення є ребрами гіперграфу системи нижчого рівня;

$g : u_{ki}^0 \cap u_{kj}^0 \to U_k^1, i \neq j$ - ребра гіперграфу більш високого рівня складності і узагальнення визначаються попарним перетином ребер гіперграфу системи нижчого рівня.

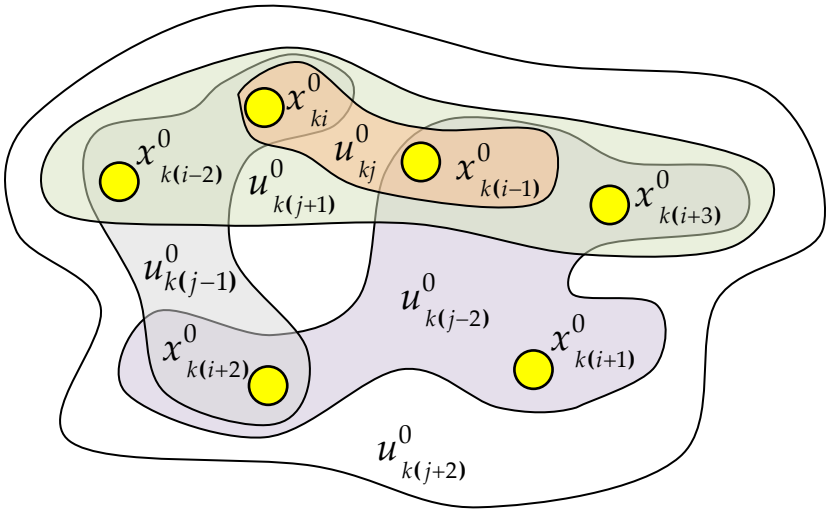

Рисунок 5 – Фрагмент гіперграфу $H_k^0(X_k^0, U_k^0)$ у k-й фазі SDLC

Для фрагменту гіперграфу $H_k^0(X_k^0, U_k^0)$ рис. 5 фрагмент гіперграфу $H_k^1(X_k^1, U_k^1)$ буде мати такі вершини і ребра:

$$X_k^1 = \left\{u^0_{k(j-2)}, u^0_{k(j-1)}, u^0_{kj}, u^0_{k(j+1)}, u^0_{k(j+2)}\right\}, \tag{3}$$

$$\begin{aligned} U_k^1 = \Big\{ & u^0_{k(j-2)} \cap u^0_{k(j-1)} = \left\{x^0_{k(i+2)}\right\}, u^0_{k(j-2)} \cap u^0_{kj} = \left\{x^0_{k(i-1)}\right\}, u^0_{k(j-2)} \cap u^0_{k(j+1)} = \left\{x^0_{k(i-1)}, x^0_{k(i+3)}\right\}, \\ & u^0_{k(j-2)} \cap u^0_{k(j+2)} = u^0_{k(j-2)}, u^0_{k(j-1)} \cap u^0_{kj} = \left\{x^0_{ki}\right\}, u^0_{k(j-1)} \cap u^0_{k(j+1)} = \left\{x^0_{k(i-2)}, x^0_{ki}\right\}, \\ & u^0_{kj} \cap u^0_{k(j+1)} = u^0_{kj}, u^0_{kj} \cap u^0_{k(j+2)} = u^0_{kj}, u^0_{k(j+1)} \cap u^0_{k(j+2)} = u^0_{k(j+1)} \Big\} \end{aligned} \tag{4}$$

Застосуємо ключові характеристики системного мислення та системного підходу до моделі мережі взаємин CITS-ISCS.

Перехід мислення від частин до цілого. Традиційно систему захисту інформації розглядають як сукупність окремих організаційних заходів і програмно-технічних засобів, визначаючі їх локальні призначення та функціональні можливості, і не роблячи, в більшості випадків, акценту на цілісність системи захисту інформації.

Уявляється необхідним в будь-якій фазі життєвого циклу системи захисту інформації:

1. описувати цільове призначення та властивості ISCS як системи без визначення складу її елементів;
2. при зосередженні уваги (створенні, оцінці/впровадженні, експлуатації, видаленні) на окремому елементі ISCS обов'язково описувати організуючі стосунки з іншими елементами, визначати місце і роль елемента в системних властивостях ISCS.

Переміщення фокусу уваги з одного рівня системи на інший. Потрібно кожен захід або засіб (елемент) ISCS розглядати як систему меншого рівня складності. Тобто, визначити властивості цього елементу як менш складної системи, яка буде мати звужену область діяльності. В ISCS необхідно визначити різницю між конфігураціями впорядкованих взаємин (паттернів) систем більшого і меншого рівня складності.

Пояснення речей в термінах зовнішнього середовища – системи більшого рівня складності. Для ISCS зовнішнім середовищем є CITS. Цілі, задачі, функції, характеристики ISCS потрібно формулювати у контексті цілей, задач, функцій, характеристик CITS. Наприклад, однією із задач ISCS може бути

забезпечення цілісності певних інформаційних ресурсів CITS. Цілісність як властивість інформації апріорі не існує, ця властивість штучно створюється власником інформації або CITS з деякою метою. Тому, формулювання задачі ISCS має бути результатом аналізу основних цільових характеристик і потреб CITS.

Перехід від пізнання об'єктів до пізнання взаємин між об'єктами. Традиційно взаємини (процеси) між складовими ISCS описуються слабо або взагалі не описуються. Відповідно до моделі мережі взаємин CITS-ISCS (рис. 4) процеси мають первинне значення, і тому обов'язково підлягають проробці і опису в контексті існування CITS. Це вже частково прописано в ISO/IEC 27001:2005 [7] у процесному підході до створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані і поліпшенні системи менеджменту захистом інформації (information security management systems, ISMS) організації.

Уявлення про наукове знання як про мережу понять і моделей, в якій ні одна частина не більш фундаментальна, ніж інша. CITS-ISCS є взаємозалежними системами, які разом формують потрібні для людини (користувача, власника інформації) властивості. Усі складові ISCS – користувачі, заходи, засоби захисту інформації та процеси між ними, є рівноправними за значенням для системи, але відрізняються один від одного як системи з різним рівнем складності. Загальна узгодженість взаємозв'язків між складовими ISCS визначає її структуру. Потрібен перенос акценту уваги в життєвому циклі ISCS на узгодженість динамічних взаємозв'язків.

Функціонування ISCS має бути не строго ієрархічне, а гібридне – поєднання ієрархічного контролю і управління із зв'язками між складовими по типу peer-to-peer (рівноправність).

Епістемологія має бути явним чином включена в опис досліджуваних феноменів. Цей підхід використовується в нормативних документах галузі захисту інформації, де регламентуються методи та засоби загальних та спеціальних досліджень при створенні та експлуатації ISCS. Тим не менш, доцільно підкреслити, що отримані результати досліджень завжди мають містити опис самого дослідника, умови, методи та засоби дослідження.

Всі наукові поняття і теорії обмежені та приблизні. Всі відомі теорії, методи, засоби та нормативні документи галузі захисту інформації обмежені та приблизні. Вони придатні тільки для обмежених умов, які в природі і суспільстві не є статичними. Розуміння цього факту дає можливість творчого (обережного) використання та застосування в конкретних умовах теорій, методів, засобів та нормативних документів галузі захисту інформації.

IV Висновки

Таким чином, використання системного мислення та системного підходу в забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем дозволило визначити формальну модель і ключові характеристики мережі взаємин CITS-ISCS.

Застосування відомих методів дослідження параметрів формальної моделі при проектуванні та експлуатації мережі взаємин CITS-ISCS дасть змогу наблизитися до створення *життєздатної* системи.

Оскільки центральним елементом CITS-ISCS є Людина, то подальшим розвитком запропонованої концепції, на думку автора, є врахування у формальній моделі мережі взаємин CITS-ISCS соціальних і біологічних аспектів діяльності Людини.

Література: ***1.*** *Ludwig von Bertalanffy, General system theory - A new approach to unity of science (Symposium), Human Biology, Dec 1951, Vol. 23, p. 303-361.* ***2.*** *Истомин Е. П., Соколов А. Г. Теория организации: системный подход. Учебник. - СПб.: ООО "Андреевский издательский дом", 2009 – 314 с.* ***3.*** *Капра Фритьоф. Паутина жизни. Новое научное понимание живых систем. Пер. с англ. под ред. В. Г. Трилиса. — К.: «София»; М.: ИД «София», 2003. — 336 с.* ***4.*** *Чу, Дж. Аналитическая теория S – матрицы. – М.: Мир, 1968, 150 с.* ***5.*** *Geoffrey F. Chew, "Bootstrap": A Scientific Idea? "Science" New Series, Vol. 161, No. 3843 (Aug. 23, 1968), pp. 762-765.* ***6.*** *NIST Special Publication 800-64 Revision 2. Security Considerations in the System Development Life Cycle [Електронний ресурс] / Stine, K.; Kissel, R.; Scholl, M.; Rossman, H.; Fahlsing, J.; Gulick, J. // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, October 2008. - Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.* ***7.*** *ISO/IEC 27001 ed1.0. Information technology - Security techniques - Information security management systems – Requirements [Електронний ресурс] // Webstore International Electrotechnical Commission, 2005-10-14. - Режим доступу: http://webstore.iec.ch/preview/info_isoiec27001{ed1.0}en.pdf.*