СПЕЦІАЛЬНІ РОЗРОБКИ

УДК 004.056:159.95

В.Л. Бурячок,
кандидат фізико-математичних наук, доцент
А.А. Шиян,
доктор технічних наук, с.н.с.

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ВІД НЕГАТИВНИХ НАСЛІДКІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Описано особливості проектування систем, застосування яких дозволить забезпечити захист людини, суспільства та держави від негативних наслідків інформаційно-психологічного впливу. Наведено ряд алгоритмів, які можуть бути покладені в основу проектування таких систем.

Ключові слова: *інформаційно-психологічна безпека, метод, негативний вплив, діяльність, система захисту.*

Описаны особенности проектирования систем, применение которых позволяет обеспечить защиту человека, общества и государства от негативных последствий информационно-психологического влияния. Приведен ряд алгоритмов, которые могут быть положены в основу проектирования таких систем.

Ключевые слова: *информационно-психологическая безопасность, метод, негативное влияние, деятельность, система защиты.*

Paper describes the features of the system design, using of which ensures the protection of an individual, society and the State from the negative effects of information and psychological influence. Series of algorithms, which can be used as the basis of the designing of such systems are described.

Keywords: *information and psychological security, method, negative influence, activity, protection system.*

Кінець XX та початок XXI століття став часом до глибинних системних перетворень у житті людей внаслідок розвитку технологій, які ще 20–30 років тому зустрічалися лише на сторінках науково-фантастичних романів. Найбільш критичними виявилися зміни, зумовлені наявністю комп'ютерів та пов'язаних із ними систем індивідуальної та спільної обробки інформації.

Якщо наприкінці XX століття великим досягненням було познайомити декілька мільйонів людей на планеті з результатами своєї діяльності (наприклад, так звані "золоті" диски співаків), то сьогодні, завдячуючи YouTube, ознайомити мільярд людей із результатами своєї творчості не становить проблеми.

Нині на людей рине гігантський потік інформації. Потік цей неврегульований, часто хаотичний та турбулентний. Останніми роками інформація, яку отримує людина,

значно збільшилася не тільки за обсягом, але й за розмаїттям сюжетів. До того ж, дуже часто така інформація є неконтрольованою. А люди в сенсі сприйняття та переробки інформації залишилися все такими ж, якими були й раніше.

Таким чином, постає актуальна в науковому плані та важлива у практичному застосуванні проблема захисту людини, суспільства та держави від негативних наслідків інформаційно-психологічного впливу. Ця задача багатогранна й потребує комплексного розв'язання.

Огляд останніх досліджень та публікацій. Описана проблема висвітлена у багатьох публікаціях вітчизняних та зарубіжних авторів. Найвідомішими з них є роботи А.В. Возженікова, В.А. Ліпкан, С.В. Ленкова, В.М. Мірошниченко, В.О. Хорошка, Ю. Курносова, П. Конотопова, В.І. Ярочкіна, К.А. Мініхена, М. Лібіцкі, О. Шермана, Д. Ешлі, Дж. Клейнберга, М. Джексона, Д. Асемоглу та інших фахівців. Тим не менш, аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексне дослідження проблеми, перш за все, у плані проектування систем інформаційно-психологічної безпеки, методів, які при цьому застосовуються, а також їх особливостей на цей час практично відсутнє. Тому, враховуючи реалії сьогодення, ця тема потребує додаткового і більш глибокого вивчення.

Метою статті є аналіз особливостей проектування систем захисту від негативних наслідків інформаційно-психологічного впливу на всіх рівнях – від людини до суспільства та держави в цілому.

Метод для інформаційно-психологічного захисту.

Спочатку зупинимося на описі методів інформаційно-психологічного впливу, які можна описати математично.

В [1, 2] побудовано формальний опис для сприйняття та переробки інформації людиною, прийняття нею рішень та здійснення діяльності.

Введено два простори: простір можливих для вибору стратегій діяльності людини I_b та простір результатів діяльності людини (результатів виконання відповідних стратегій) I_a.

Побудовано математичний апарат для моделювання діяльності людини. Для цього розроблено універсальний метод для розбиття простору I_b можливих для вибору стратегій та простору I_a результатів діяльності людини на вісім непересічних класів, які названі компонентами інформаційного простору. Таким чином, інформаційний простір I_b (та I_a) розбивається на пряму суму своїх підпросторів.

$$I_b = \sum_k \oplus I_b^k, \quad \forall k,m : I_k \cap I_m = 0 \tag{1}$$

Далі побудовано новий клас математичних операторів, що діють в цих просторах $a : I_b \to I_a$. Ці оператори названі двокомпонентними абстрактними інформаційними автоматами (2АІА). Їх мінімальна кількість становить 16 різних типів 2АІА. Кожен оператор має вигляд "чорної скриньки" $< in \mid out >$, де перший блок сприймає лише одну (задану) *програмну* компоненту інформації, а діяльність типу здійснюється в рамках іншої (заданої) *творчої* компоненти інформації.

Кожен із операторів можна задати у вигляді *впорядкованої* множини, що складається з чотирьох бінарних перемінних (які відповідають полюсам чотирьох різних дихотомій). Ця множина позначається як $\{T_i\}$. Кожен із типів 2AIA здатний при здійсненні діяльності відбирати стратегії лише з певної підмножини простору можливих стратегій I_b та здійснювати діяльність лише в рамках певної підмножини простору I_a.

В [1,2] доведено, що між типами 2AIA існують 16 взаємин, в якості яких виступають оператори переведення одного типу 2AIA в інший, та здійснено дослідження отриманої некомутативної множини автоморфізмів.

Таким чином, завдяки результатам [1,2] отримано можливість побудувати математичний інструмент для опису інформаційно-психологічного впливу на людину, що може бути покладений в основу системи проектування систем захисту від негативного впливу.

Особливості проектування систем захисту на рівні окремої людини.

Опишемо особливості проектування систем захисту від негативних наслідків інформаційно-психологічного впливу на рівні людини. Для цього буде використано описаний вище метод.

1. Предметна область діяльності людини задається характеристиками та параметрами, які мають різну природу. Однак людина, як показано в [1,2], здатна *усвідомлено* здійснювати діяльність тільки в рамках двох компонент інформації з восьми.

Внаслідок цього при проектуванні систем захисту людини необхідно всю сукупність характеристик та параметрів про предметну область діяльності (об'єкт діяльності) представити у вигляді (1). Зауважимо, що в будь-якому разі сьогодні не йдеться про *автоматичне* представлення довільної інформації у такому вигляді: поки що *селекцію* інформації буде здійснювати людина.

Алгоритм для розбиття інформації на компоненти представлено як табл. 1 [1, 2]. Алгоритм застосовується як перехід від стовпчика до стовпчика зліва направо.

Спочатку формуємо базу даних із усіх відомих характеристик предметної області. При цьому частина характеристик може бути помічена як "неінформативні" (в рамках заданої цілі) і в подальшому не розглядається.

Потім весь масив характеристик поділяється на два класи, характеристики яких наведено в табл. 1

На наступному етапі здійснюється поділ кожного із попередніх класів ще на два (опис наведено в табл. 1).

На останньому етапі кожен із чотирьох отриманих класів характеристик поділяється надвоє.

В останньому стовпчику наведено абревіатуру для назви відповідної компоненти інформації.

В результаті отримуємо вісім компонент інформації.

Таблиця 1.

Опис компонент інформаційного простору задачі для заданої цілі

Дані про об'єкт	дані про клас подібних об'єктів (узагальнюючі компоненти інформації)	опорні елементи класу (структура, топологія)	Статичність, незмінність	Ст-С
			Динамічність, мінливість	Ст-Д
		границя між даним класом і іншими	Статичність, незмінність	Гр-С
			Динамічність, мінливість	Гр-Д
	дані про саме цей об'єкт (деталізуючі компоненти інформації)	сам об'єкт як одиничний і унікальний	Статичність, незмінність	Об-С
			Динамічність, мінливість	Об-Д
		зв'язки цього об'єкта з іншими конкретними, подібними до нього	Статичність, незмінність	Зв-С
			Динамічність, мінливість	Зв-Д

Важливою обставиною є та, що такий алгоритм призводить до розбиття сукупності характеристик об'єкта дослідження, яке залежить від цілі, заради якої здійснюється створення восьмикомпонентного інформаційного простору. Таким чином, над однією й тією ж сукупністю характеристик можна створити, в загальному випадку, *декілька різних* інформаційних просторів. Тому при розробці відповідної системи захисту, тобто перед початком формування інформаційного простору, необхідно виділити та зафіксувати і предметну область, і ціль діяльності.

Наявність систем захисту, серцевиною яких є реалізація алгоритму створення інформаційного простору, дозволяє впорядкувати діяльність з інформаційно-психологічної безпеки людини за рахунок можливості *порівняння* сформованих інформаційних просторів, які здійснено людьми із *різними* типами 2AIA. Зокрема, наявність універсального алгоритму для створення інформаційного простору дозволяє здійснити порівняння різних базових елементів, які покладають аналітики з різними типами 2AIA в основу розробленого ними аналітичного продукту.

Зауважимо, що для *стандартних* ситуацій протягом деякого часу можна буде сформувати базу даних про *типові* (нормативні) інформаційні простори. Це призведе до створення банку даних вже для інформаційних просторів (які можна впорядкувати, наприклад, за предметними областями та цілями діяльності).

2. Важливе значення для проектування систем забезпечення захисту людини від шкідливого інформаційно-психологічного впливу має відповідність типу 2AIA для її діяльності тим функціональним обов'язкам, які накладаються на неї, – особливо в умовах розподілення праці (коли окрема людина здійснює лише *частину* загальної діяльності групи). Це висуває специфічні вимоги до таких систем.

По-перше, необхідно віднести *кожен* із функціональних обов'язків до певного (певних) полюсів дихотомій, які задають кожен із 16 типів 2AIA (загалом є чотири дихотомії).

По-друге, необхідно розбити множину *всіх* функціональних обов'язків на певну кількість блоків (підмножини). Кожен блок повинен бути таким, щоб його могла виконати одна людина (звичайно, кваліфікаційні вимоги теж висуваються).

Таке розбиття на блоки повинно відображувати, в загальному випадку, розподіл діяльності групи за різними предметними областями (і, можливо, за різними цілями діяльності в предметних областях). По суті, це задаються робочі місця для людини.

По-третє, необхідно вирішити *оптимізаційну* задачу щодо розподілу, описаного в попередньому пункті. В якості обмежень тут будуть виступати: набори дихотомій, які задають тип 2AIA, та обмеження на кінцеві можливості окремої людини щодо діяльності.

По-четверте, необхідно визначити умови, за якими буде агрегуватися інформація щодо кожної із дихотомій. Наприклад, це може бути сума за кожним із двох полюсів для заданого набору функціональних обов'язків: "переможна" дихотомія обирається за більшою кількістю збігів. Можна також враховувати і "ваги" для дихотомій (певної кількості чи всіх), які задаються керівником.

При формуванні інформаційно-аналітичних структур різного призначення такий алгоритм надає можливість врахувати специфічні особливості здійснення аналітичної діяльності конкретними аналітиками. Це надасть можливість, в результаті, прогнозувати *рівень якості* здійснення аналізу інформації аналітичною структурою.

3. Для спецпідрозділів міністерств оборони чи внутрішніх справ важливе значення має розробка систем захисту від шкідливого інформаційно-психологічного впливу на базі програмно-апаратних комплексів як для тренувань, так і для супроводу бійців та командирів в умовах виконання бойової задачі.

З урахуванням заданих вимог нормативних документів, ця задача зводиться до попередньої.

Проте є ще один аспект проблеми, який характерний саме для бійців спецпідрозділів.

Сьогодні залишається відкритою задача щодо наявності зв'язку між типом 2AIA людини та впливом емоційного стану в умовах бойової обстановки на рівень успішності виконання бійцем своїх функціональних обов'язків. Внаслідок цього виникає нагальна потреба щодо створення програмно-апаратних комплексів для двох *різних* задач. Перша – це дослідження рівня залежності стійкості бійців до негативного інформаційно-психологічного впливу (особливо це стосується спецпідрозділів МВС), залежно від їх типу 2AIA (причому в умовах як індивідуальної діяльності, так і діяльності у складі групи). Другою задачею є створення програмно-апаратних комплексів для *автоматичного моніторингу* стану бійців в умовах виконання бойової задачі та ідентифікації таких їх станів, які негативно впливають на її виконання. Ці програмно-апаратні комплекси доцільно інтегрувати в системи захисту від інформаційно-психологічного впливу.

4. Як показано в [1, 2], між деякими типами 2AIA існують *асиметричні* взаємини, коли інформація розповсюджується між ними *лише в один бік*. Виявлення людей, які мають такий "небезпечний" вплив на задану людину, є задачею, яка поки що не розглядається в плані *практичної реалізації*.

Проектування системи захисту від шкідливого інформаційно-психологічного впливу для виявлення серед оточення заданої людини людей, які мають "небезпечні" типи 2AIA, є сьогодні вкрай актуальною задачею. Ця задача є достатньо простою, бо вона допускає *повну математичну формалізацію* за допомогою математичного апарату, наведеного в описі методу вище в статті.

Алгоритм функціонування системи захисту формується таким чином.

Задається тип 2AIA для *виділеної* людини, яку потрібно захистити.

Задаються типи 2AIA для інших людей, які мають можливість спілкуватися із виділеною людиною.

З використанням розробленого в [1, 2] методу, із сукупності комунікантів виділяються ті люди, які можуть здійснювати негативний вплив на *виділену* людину (характеристики такого впливу можуть бути отримані за використання зазначеного методу).

Потім спілкування із такими людьми або припиняється, або ж розробляються такі спеціальні способи організації комунікації, щоб захистити *виділену* людину від шкідливого впливу.

Особливості проектування системи захисту на рівні суспільства та держави.

В [1–3] введено в науковий обіг поняття координатора як людини, що здатна або створювати *нову* інформацію, або *адекватно* доповнювати відсутню її частину. Ці люди здані виконувати діяльність на рівні управління великими суспільними структурами.

Задача ідентифікації таких людей є однією із пріоритетних для інформаційної безпеки держави насамперед тому, що *стабільність* суспільних структур та держави в цілому якраз і визначається рівнем оптимальності умов, які створені для таких людей.

В [1, 3] показано, що такі люди здатні (за певних, цілком визначених умов) створювати соціальні структури на державному рівні. За відсутності системи для ідентифікації та розміщення (ефективного використання) координаторів рівень стійкості та можливостей для розвитку суспільства та держави різко знижується.

Метод для ідентифікації координаторів базується на тому, що вони здатні пропонувати нові Проекти для виконання. Задача ідентифікації актуальна передовсім для *молодих* координаторів: вони ще не мають *виконаних* Проектів і тому можуть перебувати поза увагою відповідних суспільних та державних інститутів. За результатами ідентифікації координаторів та визначення їх рівня потрібно кожного з них *супроводжувати* протягом їх навчання з метою розміщення їх на такому місці та рівні в суспільстві, щоб вони принесли суспільству та державі максимальну користь.

Для ідентифікації координаторів доцільно використовувати спеціальні інформаційні системи, які здатні відслідковувати аналітичні матеріали, створені конкретними людьми, та співставляти їх із тими подіями, які трапляються в подальшому.

Також в якості бази даних для ідентифікації координаторів можуть виступати різноманітні конкурси, яких так багато сьогодні проводиться в Інтернеті. Однак ці Конкурси повинні бути присвячені певній темі, яка включає в себе як елемент завдання розробку Проекту для *спільної діяльності* досить великої групи людей (або ж діяльності в такій предметній області, котра включає в себе велику кількість людей чи впливає на них). Доцільно створити спеціалізовану інформаційну систему, яка могла б *супроводжувати* такі конкурси, проводячи ідентифікацію координаторів в режимі реального часу.

Підкреслимо, що клас задач із ідентифікації координаторів належить саме до рівня інформаційно-психологічної безпеки суспільства та держави. Дійсно, координатор знаходиться – як індивід, як людина та як особистість – в полі інформаційно-психологічного впливу з боку інших людей, суспільства та держави. Тому його діяльність (як мінімум – в певній частині) призводить до наслідків на рівні суспільства та держави.

Висновки.

У статті описано особливості проектування систем, застосування яких дозволить забезпечити захист людини, суспільства та держави від негативних наслідків інформаційно-психологічного впливу. Наведено ряд алгоритмів, які можуть бути покладені в основу проектування таких систем.

Описані в статті особливості проектування систем захисту є новими, вони базуються на в достатній мірі розвиненому математичному апараті, що дозволяє використовувати ці системи для вирішення широкого кола задач із забезпечення інформаційно-психологічної безпеки людини, держави та суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Шиян А.А.* Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними системами : Монографія / А.А. Шиян. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 404 с.

2. *Shiyan, Anatoliy A. and Nikiforova, Liliya O.* Types of Economic Behavior : The Instrument for Management of Individuals, Institutions, Countries and Humankind (November, 01 2011). Available at SSRN : http : // ssrn.com/abstract=1952651 or http : // dx.doi.org/10.2139/ssrn.1952651 . – 22 p. Distributed in : Information Systems : Behavioral & Social Methods eJournal, Vol 3, Issue 161, November 15, 2011.

3. *Shiyan A.A.* Management Technologies for Higher Level Officers, Presidents, Prime-Ministers and Parliamentarians // Political Behavior : Cognition, Psychology, & Behavior eJournal. – 2012. – V.6, Issue 7. – 581 p. [Electronic Resource]. – Access Mode : http : // ssrn.com/abstract=1936165 or http://dx.doi.org/10.2139/ssrn.1936165.

Отримано 6.09.2013.