© Shiyan A. Methodology of complex security for the person and social groups against the negative information-psychological influence // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 94-98.

МЕТОДОЛОГІЯ КОМПЛЕКСНОГО ЗАХИСТУ ЛЮДИНИ ТА СОЦІАЛЬНИХ ГРУП ВІД НЕГАТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Анатолій Шиян

Вінницький національний технічний університет, Україна

ШИЯН Анатолій Антонович, к.ф.-м.н.

Рік та місце народження: 1956 рік, с. Гибалівка, Вінницька область, Україна.
Освіта: Одеський державний університет ім. І.І. Мечникова, 1978 рік.
Посада: професор кафедри менеджменту та безпеки інформаційних систем з 2014 року.
Наукові інтереси: інформаційно-психологічна безпека, моделі та методи інформаційної безпеки, антитерористична діяльність.
Публікації: понад 200 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті та авторські свідоцтва.
E-mail: aa_shiyan@mail.ru

Анотація. *Інформаційно-психологічна безпека – важлива складова інформаційної безпеки держави, яка визначає захищеність громадян та суспільства від шкідливих інформаційно-психологічних впливів. Остання події у нашій державі та світі загалом вплинули на те, що забезпечення інформаційно-психологічної захищеності людини та соціальної групи визначається серед основних факторів протидії зовнішнім загрозам. У даній статті запропоновано методологію комплексного захисту людини та соціальних груп як суб'єктів інформаційної безпеки від негативного інформаційно-психологічного впливу. Вона застосовується до окремого суб'єкта, до соціальних груп (структурованих та неструктурованих), до суб'єктів, що адаптуються до організованого соціального середовища та до одно- та багаторівневих соціальних мереж.*

Ключові слова: *методологія, інформаційно-психологічний вплив, захист, суб'єкт, інформаційна безпека.*

Вступ

Стратегією національної безпеки України [1] в п. 3.1 визначена серед актуальних загроз: «інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу». Таким чином, забезпечення інформаційно-психологічної захищеності людини та соціальної групи визначається Стратегією серед основних факторів протидії зовнішнім загрозам.

Серед причин неефективності системи забезпечення національної безпеки і оборони України в п. 3.2 виділено, зокрема, що в Україні має місце «інституційна слабкість, непрофесійність, структурна незбалансованість органів сектору безпеки і оборони».

Серед заходів із забезпечення інформаційної безпеки Стратегією вимагається «удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу».

У Воєнній доктрині України [2] в п. 7 серед головних тенденцій, що впливають на воєнно-політичну обстановку в регіоні довкола України , визначена «інформаційна війна Російської Федерації проти України». А в п. 10 серед Воєнно-політичних викликів, які можуть перерости в загрозу застосування воєнної сили проти України, визначено «цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин». У п. 17 серед основних завдань воєнної політики України у найближчий час і в середньостроковій перспективі визначено, зокрема «попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованих на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні».

Стратегія кібербезпеки України [3] зазначає: «Метою Стратегії кібербезпеки України (далі – Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави». Для досягнення цієї мети пропонується, зокрема «посилення спроможностей суб'єктів сектору

безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері».

Таким чином, розробка методології комплексного захисту людини та соціальної групи від негативного інформаційно-психологічного впливу визначається цими документами як першочергове завдання.

Аналіз існуючих досліджень

Сьогодні існують декілька напрямків розробки методів захисту суб'єктів інформаційної безпеки.

Перший напрямок – це формування таких моделей суб'єкту захисту, де діяльність суб'єкта задовольняє формальним правилам [4]. Проте найбільш поширені суб'єкти захисту – люди та соціальні групи – занадто часто порушують ці формальні правила, про що переконливо свідчить феномен WikiLeaks [5].

Другий напрямок – це використання методів психології, соціології та менеджменту для управління захистом суб'єктів та протидії негативному інформаційно-психологічному впливу [6, 7]. Однак, ці методи не можуть бути ефективно застосовані до широкого кола задач інформаційної та кібербезпеки внаслідок таких причин:

- для застосування цих методів потрібно залучення вузьких спеціалістів та експертів з психології, соціології та менеджменту, що вимагає їх перенавчення для можливості їх діалогу із спеціалістами у сфері інформаційної та кібербезпеки;
- методи психології, соціології та менеджменту, як правило, базуються на суб'єктивних характеристиках діяльності суб'єкта захисту, що не дозволяє здійснити ефективну ідентифікацію інформаційного впливу та розробити ефективні методи протидії;
- методи психології, соціології та менеджменту вимагають для їх застосування обов'язкового контакту із суб'єктом захисту, що є часто неможливим для задач інформаційної та кібербезпеки, наприклад, для конкурентної розвідки чи виявлення агентів загроз.

Метою даної роботи є розробка методології комплексного захисту людини та соціальних груп як суб'єктів інформаційної безпеки від негативного інформаційно-психологічного впливу.

Основна частина дослідження

На основі результатів авторів (див., наприклад, [8-12]) розроблено методологію комплексного захисту від негативного інформаційно-психологічного впливу людини та соціальної групи як суб'єктів інформаційної безпеки, яка подана на рис. 1.

Вхідними даними методології є кортеж

$$K^{Si} =< BD^{Si}, G^{Si}, C^{Si}, AS^{Si} >, \quad (1)$$

що складається із множини G^{Si}, що задає мету діяльності суб'єкта інформаційної безпеки, множини C^{Si}, що задає обмеження на діяльність суб'єкта, множини AS^{Si}, що задає предметну область діяльності та бази даних BD^{Si}, що описує характеристики діяльності суб'єкта інформаційної безпеки. Через індекс Si позначається суб'єкт інформаційної безпеки: окремий суб'єкт CS, неструктурована соціальна група (НСГ) - NSG, структурована соціальна група (ССГ) - SSG, організоване соціальне середовище (ОСС), до якого адаптується суб'єкт - OSE, однорівнева соціальна мережа (ОСМ) - OSN, багаторівнева соціальна мережа (БСМ) - MSN.

Результатом методології є визначення заходів протидії негативного інформаційно-психологічному впливу на відповідний суб'єкт інформаційної безпеки. Її реалізація полягає у виконанні п'яти етапів.

Етап 1 – структурування інформаційного простору суб'єкта інформаційної безпеки. Виконання етапу полягає у застосуванні розробленої моделі та методу [8] структурування інформаційного простору суб'єкта, що потребує захисту від інформаційно-психологічного впливу, в якому враховуються цільові компоненти множини, що визначає діяльність суб'єкта у предметній області, а також здійснюється поетапне дихотомічне розбиття повної множини характеристик діяльності суб'єкта на вісім підмножин (враховуються дихотомічні полюси «стан – процес», «узагальнені – деталізуючі» тощо). Вхідною інформацією є кортеж (1), а вихідною – інформаційні простори (ІП) до I^{Si}_{before} та після I^{Si}_{after} здійснення діяльності відповідним суб'єктом інформаційної безпеки.

Етап 2 – формується теоретична (зразкова) база даних результатів діяльності відповідного суб'єкта інформаційної безпеки.

Теоретична база даних результатів діяльності визначається за формулою

$$R^{Si}_e = I^{Si}_{after} - I^{Si}_{before}. \quad (2)$$

У (2) значення I_{after} береться із етапу 1 як теоретичне (прогнозне) значення ІП, яке отримується після здійснення заданої діяльності відповідним суб'єктом інформаційної безпеки Si.

У залежності від вибору суб'єкта Si, результуюча база даних R^{Si}_e формується таким чином.

Для $Si = CS$ вхідними даними є K^{CS} K^{CS}, а вихідними – R^{CS}_e.

Для $Si = NSG$ вхідними даними є K^{NSG} та R^{CS}_e, а вихідними – R^{NSG}_e.

Для $Si = SSG$ вхідними даними є K^{SSG}, R^{CS}_e та R^{NSG}_e, а вихідними – R^{SSG}_e.

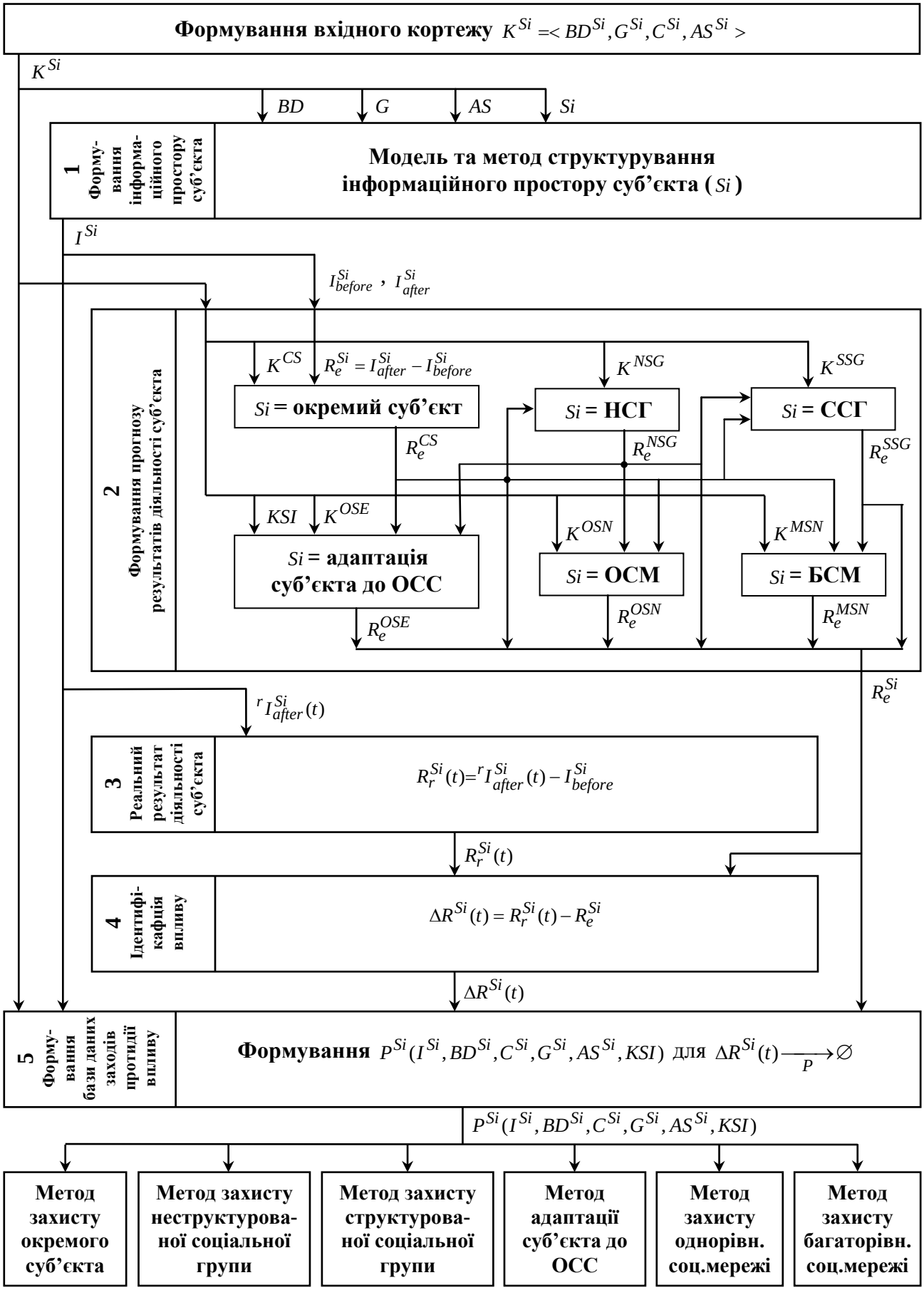

Рис. 1. Методологія комплексного захисту від негативного інформаційно-психологічного впливу людини та соціальної групи як суб'єктів інформаційної безпеки

Для $Si = OSE$ вхідними даними є KSI, K^{OSE}, R_e^{CS}, та R_e^{NSG}, а вихідними – R_e^{OSE}.

Для $Si = OSN$ вхідними даними є код соціального інститут для ОСР K^{OSN}, R_e^{CS} та R_e^{NSG}, а вихідними – R_e^{OSN}.

Для $Si = MSN$ вхідними даними є K^{MSN}, R_e^{CS} та R_e^{SSG}, а вихідними – R_e^{MSN}.

Таким чином, вхідними для більшості суб'єктів є теоретичні (прогнозні) бази даних результатів діяльності деяких інших суб'єктів. Детально цей етап подано в [8 – 11].

Етап 3 – формується база даних реальних (дійсних) результатів діяльності визначеного суб'єкта на даний момент часу. На даному етапі визначаються за формулою (3) база даних реальних результатів діяльності, що здійснена відповідним суб'єктом інформаційної безпеки

$$R_r^{Si}(t) = {}^{r}I_{after}^{Si}(t) - I_{before}^{Si}. \quad (3)$$

Вхідними характеристиками є тип суб'єкта інформаційної безпеки Si, інформаційний простір ${}^{r}I_{after}^{Si}$ цього суб'єкта, що формується на даний час із бази даних реальних характеристик після здійснення його діяльності, та ІП даного суб'єкта I_{before}^{Si}, який побудовано до початку діяльності.

Для випадку НСГ детально метод подано в [12].

Етап 4 – формується база даних відмінностей реальних результатів визначеного суб'єкта від прогнозних на заданий момент часу. Ця база даних (вихідні характеристики етапу) визначається за формулою (4)

$$\Delta R^{Si}(t) = R_r^{Si}(t) - R_e^{Si}. \quad (4)$$

Вхідними характеристиками етапу слугують вихідні характеристики етапів 3 та 2, тобто, відповідно, база даних характеристик реальних результатів $R_r^{Si}(t)$ діяльності суб'єкта та база даних теоретичних характеристик R_e^{Si} діяльності цього суб'єкта.

Цей етап подано в [8 – 13].

Етап 5 – розробка заходів для протидії інформаційно-психологічному впливу на визначений суб'єкт інформаційної безпеки. Вихідними характеристиками є база даних заходів протидії $P^{Si}(I^{Si}, BD^{Si}, C^{Si}, G^{Si}, AS^{Si}, KSI)$, яка залежить від інформаційного простору суб'єкта I^{Si}, бази даних діяльності суб'єкта BD^{Si}, обмежень на діяльність суб'єкта C^{Si}, цілі діяльності суб'єкта G^{Si}, предметної області діяльності суб'єкта AS^{Si} та, за потреби, від класу ОСС KSI. Знаходиться ця база із задачі на оптимізацію

$$\Delta R^{Si}(t) \xrightarrow[P]{} \varnothing. \quad (5)$$

Вхідними характеристиками є вхідні характеристики попередніх етапів (див. [8-13]).

Приклад реалізації методології для випадку усунення інформаційної пробки в НСГ подано в [13].

Обговорення результатів

В статті вперше розроблено методологію комплексного захисту людини та структурованих і неструктурованих соціальних груп з врахуванням можливості адаптації окремих суб'єктів, що потребують захисту, та їх груп до організованого соціального середовища, а також одно- та багаторівневих соціальних мереж від негативного інформаційно-психологічного впливу, яка враховує класи характеристик діяльності окремого суб'єкта та скінченну множину класів бінарних відношень між цими суб'єктами з використанням визначених операторів, що дозволило забезпечити захист різного роду суб'єктів та суб'єктних груп від негативного інформаційно-психологічного впливу.

Висновки

У статті запропонована методологія комплексного захисту людини та соціальних груп як суб'єктів інформаційної безпеки від негативного інформаційно-психологічного впливу. Вона застосовується до окремого суб'єкта, до соціальних груп (структурованих та неструктурованих), до суб'єктів, що адаптуються до організованого соціального середовища та до одно- та багаторівневих соціальних мереж. Запропоновану методологію може бути покладено в основу розробки широкого кола методів та засобів для захисту суб'єктів інформаційної безпеки від негативного інформаційно-психологічного впливу, що дозволяє використовувати її для розробки потужних інструментів кібербезпеки.

Література

[1] Стратегія національної безпеки України. Указ Президента України №287/2015 від 26 травня 2015 р. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015

[2] Воєнна доктрина України. Указ Президента України № 555/2015 від 24 вересня 2015 р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/555/2015

[3] Стратегія кібербезпеки України. Указ Президента України № 96/2016 від 15 березня 2016 р.

[4] Богуш В.М. Теоретичні основи захищених інформаційних технологій / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.

[5] Ассанж Дж. Неавторизированная автобиграфия / Дж. Ассанж. – М.: Альпина Бизнес Букс, 2012. – 264 с.

[6] Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

[7] Андреєв В.І. Стратегія управління інформаційною безпекою / В.І. Андреєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К. : ДУІКТ, 2007. – 277 с.

[8] Шиян А.А. Теоретико-ігровий аналіз раціональної поведінки людини та прийняття рішень в управлінні соціально-економічними

системами / А.А. Шиян. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 404 с.

[9] Шиян А.А. Управління формуванням ефективних економічних інститутів для України / А.А. Шиян, Л.О. Нікіфорова. – Вінниця: ВНТУ, 2011. – 300 с.

[10] Шиян А.А. Методи та технології захисту людини від негативного інформаційно-психологічного впливу / А.А. Шиян // Інформаційна безпека. – 2013. – №3 (11). – С. 98-104.

[11] Яремчук Ю.Є. Метод оптимізації діяльності неструктурованої групи експертів в умовах ліквідації надзвичайних ситуацій / Ю.Є. Яремчук, Л.О. Нікіфорова, А.А. Шиян // Реєстрація, зберігання і обробка даних. – 2015. – Т.17, №4. – С. 59-70.

[12] Шиян А.А. Модель та методи захисту структурованої соціальної групи від негативного інформаційно-психологічного впливу / Ю.Є. Яремчук, А.А. Шиян // Захист інформації. – 2014. – Т.16, №4. – С. 311-317.

[13] Яремчук Ю.Є. Метод оптимізації діяльності неструктурованої групи експертів в умовах ліквідації надзвичайних ситуацій / Ю.Є. Яремчук, Л.О. Нікіфорова, А.А. Шиян // Реєстрація, зберігання і обробка даних. – 2015. – Т.17, №4. – С. 59-70.

УДК 004.056:159.95 (045)

Шиян А.А. Методология комплексной защиты человека и социальных групп от негативного информационно-психологического влияния

Аннотация. *Информационно-психологическая безопасность – важная составляющая информационной безопасности государства, которая определяет защищенность граждан и общества от вредных информационно-психологических воздействий. Последние события в нашей стране и мире в целом повлияли на то, что обеспечение информационно-психологической защищенности человека и социальной группы определяется среди основных факторов противодействия внешним угрозам. В статье предложена методология комплексной защиты человека и социальных групп как субъектов информационной безопасности от негативного информационно-психологического влияния. Она применяется к отдельному субъекту, к социальным группам (структурированным и неструктурированным), к субъектам, которые адаптируются к организованной социальной среде и к одно- и многоуровневым социальным сетям.*

Ключевые слова: *методология, информационно-психологическое влияние, защита, субъект, информационная безопасность.*

Shiyan A. Methodology of complex security for the person and social groups against the negative information-psychological influence

Abstract. *Information and psychological security is an important component of information security, which determines the security of citizens and society from harmful information and psychological influences. The latest events in our country and around the world affected by the fact that the provision of information and psychological security of person and social group defined among the main factors countering external threats. The paper proposes a methodology for comprehensive security for human and social groups as the subjects of information security from negative information-psychological impact. It applies to an individual subject, to social groups (structured and unstructured), to the subjects, which are adapted to the organized social environment, and to the single and multi-level social networks.*

Key words: *methodology, information-psychological influence, security, subject, information security.*

Отримано *15 лютого 2016 року*, затверджено редколегією *4 березня 2016 року*