Вісник Львівського університету. Серія філос.-політолог. студії. 2023. Випуск 49, с. 278–285
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 49, p. 278–285

УДК 681.3
DOI https://doi.org/10.30970/PPS.2023.49.34

ОСНОВНІ ПІДХОДИ ДО РОЗУМІННЯ «КОГНІТИВНА БЕЗПЕКА» В СУЧАСНІЙ НАУЦІ: ПОЛІТИЧНИЙ ТА ІНФОРМАЦІЙНИЙ АСПЕКТ

Тарас Кобець
Прикарпатський національний університет імені Василя Стефаника,
факультет історії, політології і міжнародних відносин, кафедра політології
вул. Шевченка, 57, 76000, м. Івано-Франківськ, Україна
https://orcid.org/0009-0001-2179-321X

У сучасному світі важливість когнітивної безпеки має серйозні наслідки. Зростаюча кількість дезінформації, фейків та кіберзагроз підриває надійність інформаційного оточення. Люди стають вразливими перед маніпуляціями, втрачаючи здатність критично мислити. Це може спричинити поширення помилкових поглядів, поглибити політичні та суспільні розколи. Відсутність адекватної когнітивної безпеки впливає на прийняття рішень, схильність до популізму та радикалізацію. Ослаблюється довіра до ЗМІ та інституцій, загрожуючи стабільності суспільства. Запобігання вадливості когнітивної безпеки важливо для забезпечення інформаційної безпеки та збереження демократичних цінностей.

Забезпечення когнітивної безпеки в рамках загальної безпеки держави є невід'ємною складовою сучасного світу. Розвиток інформаційних технологій призводить до появи нових загроз, включаючи дезінформацію, кібератаки та маніпуляції. Забезпечення когнітивної безпеки означає підготовку та освіту громадян, які здатні критично оцінювати інформацію, розпізнавати дезінформацію та захищати себе від кіберзагроз. Це важливо для зміцнення національної безпеки, підтримання довіри громадян до державних інституцій та забезпечення стабільності суспільства. Крім того, когнітивна безпека сприяє ефективній інформаційній взаємодії між державою та громадянами, що є важливим елементом сучасного управління та забезпечення національної безпеки.

Когнітивна безпека стає надзвичайно важливою в умовах гібридних воєн, де використовуються не тільки військові, а й інформаційні, політичні та економічні методи для досягнення своїх цілей. У таких умовах дезінформація, психологічний тиск та кібератаки можуть бути ефективними інструментами впливу. Забезпечення когнітивної безпеки передбачає підготовку громадян до аналізу та розпізнавання маніпуляцій, вміння розрізняти факти від дезінформації, а також здатність до критичного мислення. Це допомагає зменшити вплив гібридних загроз, зміцнює стійкість суспільства та підвищує національну безпеку. Когнітивна безпека в гібридних війнах оберігає від маніпуляцій, зміцнює резистентність суспільства та сприяє інформаційній безпеки.

Ключові слова: когнітивна безпека, інформаційна безпека, безпека, безпека держави.

Вступ. Зростаюча роль когнітивних факторів у формуванні публічної думки, прийнятті політичних рішень та сприйнятті інформації наголошує на необхідності глибокого аналізу концепту «когнітивна безпека». З'ясування політичних та інформаційних аспектів цієї концепції сприяє розробці стратегій протидії маніпуляціям, дезінформації та когнітивним загрозам. Отже, вивчення даної проблематики сприяє поглибленому розумінню сучасних викликів та розвитку ефективних заходів для забезпечення стабільності і безпеки суспільства.

Розуміння впливу когнітивних аспектів на соціальні процеси є важливим у контексті змін у медіа-середовищі та інформаційних технологіях. Вивчення концепту «когнітивна безпека» дозволяє не лише розкрити психологічні механізми сприйняття інформації, але

й розробити підходи до вдосконалення медіа-грамотності та критичного мислення громадян. Аналіз політичних та інформаційних вимірів концепції допомагає створити відповідні стратегії для запобігання маніпуляціям та впливовій пропаганді. Це важливий крок у забезпеченні стійкої інформаційної екосистеми та збереженні соціальної гармонії, о і обумовлює актуальність тематики даної роботи.

Постановка проблеми. Сучасне інформаційне середовище викликає необхідність ретельного розгляду проблеми когнітивної безпеки. Зростаюча важливість когнітивних факторів у формуванні думок і прийнятті політичних рішень вказує на актуальність вивчення впливу інформаційного втручання на ці процеси. Розробка ефективних стратегій захисту від маніпуляцій та збереження стабільності суспільства стає важливою задачею у цьому контексті.

Швидка та масштабна поширеність інформації у суспільстві підвищує ризик впливу маніпулятивних стратегій на свідомість та рішення людей. Встановлення взаємозв'язку між когнітивними процесами та впливом інформації на них є нагальним завданням. Необхідність розробки превентивних заходів, спрямованих на захист від дезінформації та маніпуляцій, стає очевидною. Дослідження цієї проблематики розкриє важливі аспекти взаємодії інформаційного середовища та когнітивних механізмів, сприяючи стійкому та раціональному розвитку суспільства.

Аналіз останніх досліджень та публікацій. Питанням дослідження категорії «когнітивна безпека» присвячена значна кількість наукових робіт вітчизняних вчених. Так Л. Бєлкін досліджував співвідношення понять «інформаційна безпека»,» безпека інформації»,» та «когнітивна безпека». В той же час Зубар Н. розглядав «когнітивну безпеку» України в контексті повномасштабного вторгнення рф.

В той же час Коваль З. займався вивченням психологічних механізмів та впливу війн та операцій на історичні події та сучасне суспільство. В свою чергу Журибіда Н. Р. аналізував цільові орієнтири та функціональних аспектів, пов'язаних з економічною безпекою банків. Спасителева С. досліджувала проблеми безпеки універсальних платформ управління даними.

В своїй роботі Топчій О. вивчала різні види інформаційної безпеки щодо неповнолітніх та нові підходи до цієї проблеми.

Автюзенко О. В свої роботі розглядає методи, способи та інструменти теорії прийняття рішень для моделювання систем захисту інформації на різних рівнях. Робота Москаленко В. В. присвячена дослідженню особливості когнітивного компоненту творчого мислення при вирішенні над ситуативних проблем.

В той же час Богданович В. досліджував можливість розробки методу когнітивного моделювання негативного впливу гібридних загроз на національну безпеку держави. В свою чергу Дергильова О. досліджувала розробки моделі науково-технічної сфери системи забезпечення воєнної безпеки держави.

Салієва О. В. досліджувала розробку когнітивної моделі для визначення рівня захищеності об'єкта критичної інфраструктури. Гаценко С. займалася моделюванням процесу визначення загроз воєнній безпеці як складової національної безпеки держави.

Постановка завдання. Метою даної статті є систематизація теоретичних знань щодо підходів до розуміння категорії «когнітивна безпека».

Викладення основного матеріалу. Когнітивна безпека стає дедалі важливішою в сучасному світі, де інформаційні технології проникають у всі сфери життя. Ця концепція відноситься до захисту індивідів від маніпуляцій, дезінформації та кіберзагроз, спрямованих на їхнє мислення і пізнавальні процеси.

Важливість когнітивної безпеки полягає в тому, що недостатній захист може призвести до прийняття неправильних рішень, спотворення світогляду та підриву довіри до інформації. Засоби захисту включають критичне мислення, медійну грамотність та усвідомлення психологічних механізмів впливу. Забезпечення когнітивної безпеки допомагає громадянам бути більш обізнаними, самостійними та раціональними споживачами інформації в цифровому вікові.

Взаємозв'язок між когнітивною безпекою та безпекою держави надзвичайно важливий. Когнітивна безпека нації залежить від здатності громадян критично оцінювати інформацію, уникати дезінформації та кіберзагроз. Це впливає на політичну стабільність та внутрішню єдність держави. Спотворена або невірна інформація може стати інструментом гібридних загроз, руйнації національної безпеки та міжнародних відносин. Дбайливе ставлення до когнітивної безпеки сприяє зміцненню національної безпеки та резистентності суспільства перед загрозами.

Когнітивна безпека формує свідомих громадян, що здатні розпізнавати маніпуляції, забезпечуючи стійкість інформаційного простору та загальну стійкість держави перед внутрішніми та зовнішніми загрозами.

На сьогоднішній день не існує єдиного визначення категорії «когнітивна безпека», зважаючи на це існує необхідність розкриття та аналізу існуючих визначень даної категорії, для чого скористаємося нижченаведеною таблицею (Таблиця 1), в якій наочним чином відображені дані автори та їх трактування категорії.

Враховуючи вищенаведені визначення, можна підсумувати, що когнітивна безпека представляє собою комплексний підхід до забезпечення стійкості індивідів та суспільства від інформаційно-психологічних впливів. Це поняття включає в себе заходи та стратегії, спрямовані на захист когнітивних процесів, інтелектуальних зусиль та психологічного благополуччя в умовах зростаючого впливу цифрових технологій і онлайн-середовищ. Когнітивна безпека фокусується на розпізнаванні, аналізі та протидії загрозам, пов'язаним з маніпулюванням когнітивними процесами, такими як мислення, сприйняття, увага та прийняття рішень. Її метою є гарантування надійності та безпеки інтелектуальних систем,

Таблиця 1

Визначення категорії «когнітивна безпека» в працях сучасних науковців

№ п/п	Автор	Визначення
1	Бєлкін Л. М. [1]	Когнітивна безпека – це стійкість проти інформаційно-психологічних впливів на людину і суспільство.
2	Рущенко І. П. [1]	Когнітивна безпека – загрози й ризики, які пов'язані з пізнавальною діяльністю, негативними впливами мас-медіа, перебуванням людини у віртуальній реальності.
3	Зубар Н. [2]	Когнітивна безпека – це концепція, що охоплює заходи та стратегії для захисту когнітивних процесів, інтелектуальних зусиль та психологічного благополуччя в особистому та колективному сприйнятті і обробці інформації, які можуть бути піддані загрозам або зловживанню, зазвичай у контексті цифрових технологій та онлайн-середовищ.
4	Коваль З. [3]	Когнітивна безпека зосереджується на виявленні, аналізі та протидії загрозам, пов'язаним з маніпуляціями когнітивними процесами, такими як мислення, сприйняття, увага та прийняття рішень. Метою когнітивної безпеки є забезпечення надійного та безпечного функціонування інтелектуальних систем, запобігання впливу зловживань та злочинної діяльності, а також збереження довіри та прозорості в застосуванні штучного інтелекту та його впливу на суспільство.

запобігання зловживанням та кримінальній діяльності, а також збереження довіри та прозорості в використанні штучного інтелекту та його впливу на суспільство. Це поняття актуальне через зростаючий вплив технологій на наші пізнавальні процеси та спосіб сприйняття інформації.

Когнітивна безпека у сучасних умовах орієнтується на захист когнітивних процесів, інтелектуальної діяльності та психологічного благополуччя індивідів і суспільства від впливів, що можуть спотворити перспективи та оцінки, спричинити маніпуляції та зловживання інформацією. Когнітивна безпека реалізується через розвиток критичного мислення, підвищення обізнаності щодо маніпулятивних та дезінформаційних практик, а також розуміння психологічних механізмів впливу на сприйняття та рішення.

У зв'язку з поширеністю цифрових технологій та збільшенням кількості інформації, до якої мають доступ індивіди, когнітивна безпека стає надзвичайно важливим елементом забезпечення інформаційної безпеки держави. Вона забезпечує усвідомлене та обґрунтоване використання інформації, а також реакцію на загрози та виклики, що мають психологічний та інформаційний вимір.

На нижченаведеному рисунку (Рисунок 1) наочним чином відображено місце когнітивної безпеки в загальній структурі (системі) інформаційної безпеки.

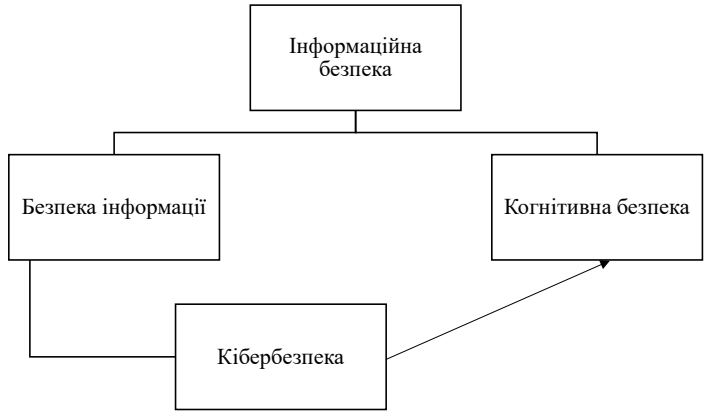

Рис. 1. Когнітивна безпека в структурі інформаційної безпеки [1]

Когнітивна безпека, як важлива складова інформаційної безпеки, впливає на ефективність та стійкість всієї інформаційної системи, включаючи кібербезпеку. Основні аспекти включають:

- розпізнавання загроз;
- протидія дезінформації;
- забезпечення довіри;
- збереження психологічної стійкості;
- попередження впливу кібератак;
- збереження ефективності заходів кібербезпеки.

Отже, когнітивна безпека виступає як важлива ланка інформаційної безпеки, покликана захищати не лише технічні компоненти систем, але й психологічний стан, мислення та сприйняття користувачів, забезпечуючи збалансований та стійкий розвиток суспільства в інформаційній епохі.

Слід зауважити що поняття «когнітивна безпека» є багатогранним, через що виникає необхідність сегментації даної категорії в рамках різних підходів (Рисунок 2).

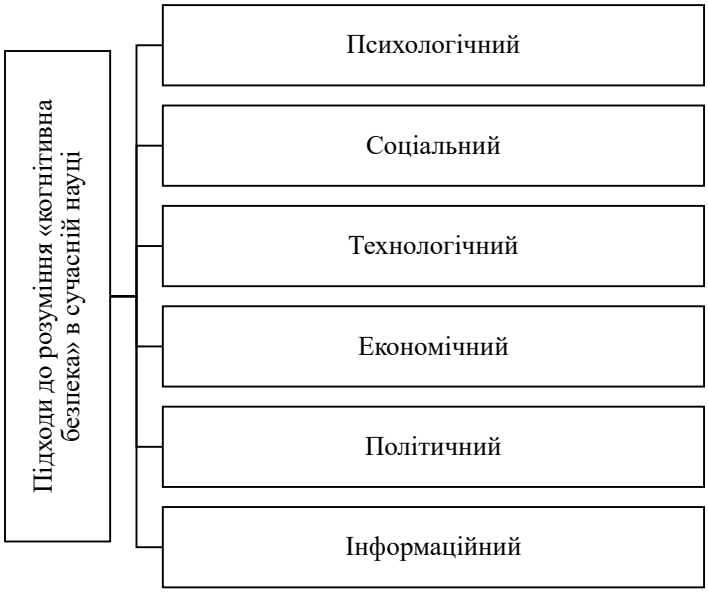

Рис. 2. Підходи до розуміння «когнітивна безпека» в сучасній науці

Джерело: побудовано автором за [1–12]

Психологічний підхід до розуміння когнітивної безпеки в сучасній науці акцентує увагу на взаємозв'язку між інформаційними впливами та психічним станом індивіда. Цей підхід спрямований на розпізнавання та захист когнітивних процесів від маніпуляцій, забезпечуючи психологічну стійкість та об'єктивне сприйняття інформації.

Соціальний підхід в сучасній науці аналізує вплив інформаційних процесів на суспільство та міжособистісні взаємодії. Він розглядає вплив мас-медіа, соціальних мереж та інших комунікаційних каналів на психологічний стан та сприйняття індивідів, а також їхню здатність формувати колективну думку. Цей підхід спрямований на розуміння взаємозв'язку між інформаційними впливами та суспільною динамікою, а також вироблення стратегій захисту від маніпуляцій та дезінформації.

Технологічний підхід відносно розуміння когнітивної безпеки в сучасній науці акцентує увагу на ролі сучасних інформаційних технологій у формуванні та забезпеченні безпеки когнітивних процесів. Цей підхід розглядає застосування штучного інтелекту, аналітичних алгоритмів та додатків для розпізнавання погроз, фільтрації дезінформації та підвищення інформаційної грамотності. Технологічний підхід визначає методи захисту від маніпулятивних впливів у віртуальному середовищі та сприяє розвитку кібербезпеки з урахуванням психологічних аспектів користувачів.

Економічний підхід в сфері когнітивної безпеки акцентує увагу на взаємозв'язку між заходами захисту когнітивних процесів та економічними аспектами. Цей підхід досліджує вплив маніпуляцій на рівень довіри, споживчу поведінку та інвестиційний клімат, а також розглядає витрати на протидію інформаційним загрозам і дезінформації.

Політичний підхід до розуміння когнітивної безпеки у сучасній науці аналізує взаємодію інформаційних впливів та політичних процесів. Він вивчає роль маніпуляцій та дезінформації в політичних кампаніях, вплив цифрових засобів на формування громадської думки та підтримку певних політичних поглядів. Політичний підхід аналізує можливість використання інформаційних впливів для досягнення політичних цілей, а також розробляє стратегії захисту когнітивних процесів від негативних політичних маніпуляцій.

Інформаційний підхід щодо когнітивної безпеки в сучасній науці визначається як розгляд впливу інформаційних засобів на когнітивні процеси та психологічний стан індивідів. Цей підхід досліджує роль мас-медіа, цифрових платформ, а також соціальних мереж у формуванні сприйняття, переконань та рішень людей.

Інформаційний підхід допомагає розуміти, які інформаційні впливи можуть спотворити об'єктивний сприйняття дійсності та спричинити психологічний вплив на індивідів, а також розробляє методи захисту когнітивних процесів від негативних інформаційних маніпуляцій.

Забезпечення когнітивної безпеки України у контексті воєнного вторгнення рф набуває вищої важливості для збереження національної суверенності та стабільності суспільства. Військовий конфлікт підсилює використання маніпулятивних та дезінформаційних технік для впливу на сприйняття, образ ворога, мобілізацію населення та дестабілізацію держави. Забезпечення когнітивної безпеки включає розвиток інформаційної грамотності громадян, виявлення дезінформації, підвищення обізнаності щодо психологічних механізмів впливу. Це не лише підвищує стійкість суспільства перед інформаційними загрозами, але й сприяє підтримці національної єдності та довіри до інформаційних джерел під час кризових ситуацій.

Висновки. Як підсумок даної науково-дослідної роботи можна зробити наступні висновки:

1. Термін «когнітивна безпека» визначається як концептуальна парадигма, що охоплює заходи та стратегії для захисту когнітивних процесів та інтелектуальної діяльності в особистому та колективному сприйнятті і обробці інформації. Цей підхід акцентує на виявленні, аналізі та протидії загрозам, пов'язаним з маніпуляціями когнітивними процесами, що можуть спотворити об'єктивне сприйняття дійсності та призвести до психологічного впливу на індивіда. Метою когнітивної безпеки є забезпечення стійкого та безпечного функціонування інтелектуальних систем, попередження зловживань, збереження довіри та прозорості в інформаційному середовищі.

2. Аналіз підходів до визначення когнітивної безпеки свідчить про її комплексний характер та важливість у сучасному інформаційному суспільстві. Психологічний підхід акцентує на психічному стані індивіда, соціальний – на впливі на громадську думку, технологічний – на застосуванні штучного інтелекту, економічний – на витратах та політичний – на впливі на політичні процеси. Інформаційний підхід розглядає роль інформаційних засобів. Ці підходи взаємопов'язані та доповнюють один одного, створюючи фундамент для ефективного забезпечення когнітивної безпеки в різних сферах життя суспільства.

Список використаної літератури

1. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» як стійкість проти інформаційно психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір*: Матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р. С. 195–197.

2. Зубар Н., Рущенко, І. П. Когнітивна зброя і когнітивна безпека: постановка питання. *Українське суспільство в умовах війни: виклики сьогодення та перспективи*. 2017. С. 267–270.
3. Коваль З. Психоісторичні операції та війни як засіб управління минулим і сьогоденням: механізми правової протидії. *Актуальні проблеми державного управління*. 2018. Вип. 2. С. 79–84.
4. Журибіда Н. Р. Цільові орієнтири та функціональні аспекти економічної безпеки банків. *Вісник Одеського національного університету. Серія: Економіка*. 2019. Вип. 24(4). С. 123–127.
5. Spasiteleva S., Zhdanova Y., & Chychkan I. Проблеми безпеки універсальних платформ управління даними. «*Кібербезпека: освіта, наука, техніка*». 2019. Вип. 2(6). С. 1. Spasiteleva S., Zhdanova Y., Chychkan I. Security problems of universal data management systems. *Cybersecurity: Education, Science, Technique*. 2019. Vol. 2, № 6. P. 122–133. URL: https://doi.org/10.28925/2663-4023.2019.6.122133 (date of access: 01.09.2023).
6. Топчій О. Види інформаційної безпеки неповнолітніх: новий погляд на усталені підходи. *Jurnalul juridic national: teorie şi practică*. 2019. Вип. 35(1). С. 122–126.
7. Analysis of methods, methods, mechanisms, tools theories of decision-making for modeling information protection system / O. Avtushenko et al. *Cybersecurity: Education, Science, Technique*. 2022. Vol. 16, № 4. P. 159–171. URL: https://doi.org/10.28925/2663-4023.2022.16.159171 (date of access: 01.09.2023).
8. Москаленко В. В. Особливості когнітивного компоненту творчого мислення в процесі розв'язання суб'єктом надситуативної проблемності. *Актуальні проблеми психології*. 2019. Том УІ: Психологія обдарованості.-Вип. 15. С. 107–113.
9. Богданович В., Олексіюк В., Павліковський А., Передрій О., Муженко, В. Метод когнітивного моделювання негативного впливу гібридних загроз на національну безпеку держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2023. № 1(77). С. 6–12.
10. Дергильова О. Модель науково-технічної сфери системи забезпечення воєнної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. Вип. 40(1). С. 175–180.
11. Салієва О. В., Яремчук Ю. Є., Салиева О. В., & Яремчук Ю. Е. Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури. *Безпека інформації*. 2020. Т. 26, № 2. С. 64–73.
12. Гаценко С., Пащенко К., Сверединок Ю., Стариш М. Модель процесу визначення загроз воєнній безпеці, як складової національної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. № 42(3). С. 111–116.

MAIN APPROACHES TO UNDERSTANDING "COGNITIVE SECURITY" IN MODERN SCIENCE: POLITICAL AND INFORMATIONAL ASPECTS

Taras Kobets
Vasyl Stefanyk Precarpathian National University,
Faculty of History, Politology and International Relations, Department of Politology
Shevchenka str., 57, 76000, Ivano-Frankivsk, Ukraine
https://orcid.org/0009-0001-2179-321X

In the modern world, the importance of cognitive security has serious consequences. A growing number of disinformation, fakes and cyber threats undermine the reliability of the information environment. People become vulnerable to manipulation, losing their ability to think critically. This can lead to

the spread of false views and deepen political and social divisions. Lack of adequate cognitive security affects decision-making, susceptibility to populism and radicalisation. Trust in the media and institutions is weakened, threatening the stability of society. Preventing cognitive security flaws is important for ensuring information security and preserving democratic values.Ensuring cognitive security as part of the overall security of the state is an integral part of the modern world. The development of information technology leads to the emergence of new threats, including disinformation, cyberattacks and manipulation. Ensuring cognitive security means training and educating citizens who are able to critically evaluate information, recognise disinformation and protect themselves from cyber threats. This is important for strengthening national security, maintaining public trust in state institutions, and ensuring the stability of society. In addition, cognitive security promotes effective information interaction between the state and citizens, which is an important element of modern governance and national security. Cognitive security becomes extremely important in hybrid wars, where not only military, but also information, political and economic methods are used to achieve their goals. In such circumstances, disinformation, psychological pressure and cyber attacks can be effective tools of influence. Ensuring cognitive security involves preparing citizens to analyse and recognise manipulations, the ability to distinguish facts from disinformation, and the ability to think critically. This helps to reduce the impact of hybrid threats, strengthens the resilience of society and enhances national security. Cognitive security in hybrid warfare protects against manipulation, strengthens society's resilience, and promotes information security.

Key words: cognitive security, information security, security, state security.