УДК 004.056:351.861
DOI: 10.25140/2411-5363-2020-4(22)-96-108

Юлія Ткач

КОНЦЕПТУАЛЬНА МОДЕЛЬ БЕЗПЕКИ КІБЕРПРОСТОРУ

Актуальність теми досліджень. *Державні інформаційні ресурси й засоби здійснення електронних мережевих транзакцій (сервери, маршрутизатори, сервери вилученого доступу, канали зв'язку, операційні системи, бази даних і додатки) потрібно захищати особливо надійно і якісно. Це зумовлено тим, що вартість наслідків кожного «зламу» захисту швидко росте й це буде тривати в найближчому майбутньому.*

Постановка проблеми. *Забезпечення інформаційної безпеки мереж і систем обробки є пріоритетним завданням для керівництва держави, оскільки від збереження конфіденційності, цілісності й доступності державних інформаційних ресурсів багато в чому залежить якість та оперативність прийняття стратегічних рішень та ефективність їхньої реалізації.*

Аналіз останніх досліджень і публікацій. *Попри постійно зростаючу кількість публікацій, присвячених інформаційній безпеці, проблема забезпечення безпеки в кіберпросторі, особливо держави, залишається невирішеною.*

Виділення недосліджених частин загальної проблеми. *Нині в роботах вітчизняних та закордонних учених недостатньо уваги приділено розробці систем та моделей кібербезпеки держави.*

Постановка завдання. *Метою статті є побудова концептуальної моделі безпеки в межах кіберпростору, що опише складові національної кібербезпеки та дозволить встановити силу зв'язку між відповідними її складовими, а також визначити рівень кібербезпеки.*

Виклад основного матеріалу. *З використанням діаграм Ейлера-Венна графічно представлено кіберпростір держави та на основі теорії множин запропоновано більш строгий опис моделі. У загальному вигляді концептуальна модель безпеки кіберпростору формується на основі трьох компонентів: особи, яка обробляє інформацію, володіє нею або здійснює її захист; нормативно-правові акти, які забезпечують юридичний захист інформації; інформаційні ресурси, у яких сконцентровано інформацію, що потребує захисту, і в межах яких функціонують засоби захисту інформації.*

Висновки відповідно до статті. *У статті побудовану концептуальну модель безпеки держави, що описує складові кібербезпеки держави та дозволяє встановити силу зв'язку між відповідними її складовими, а також визначити рівень кібербезпеки.*

Ключові слова: *кіберпростір; концептуальна модель; інформаційна безпека держави; безпека інформації.*
Рис.: 6. Табл.: 2. Бібл.: 9.

Актуальність теми дослідження. Використання кіберпростору держави як глобальної публічної мережі означає для засобів безпеки об'єктів захисту не тільки різке збільшення кількості зовнішніх користувачів і розмаїтість типів комунікаційних зв'язків, але і співіснування з новими мережевими й інформаційними технологіями. Тому інформаційні ресурси та засоби здійснення електронних мережевих транзакцій (сервери, маршрутизатори, сервери вилученого доступу, канали зв'язку, операційні системи, бази даних і додатки) потрібно захищати особливо надійно і якісно. Це зумовлено тим, що вартість наслідків кожного «зламу» захисту швидко росте й це буде тривати в найближчому майбутньому.

Постановка проблеми. Засоби зламу мереж і розкрадання інформації розвиваються так само швидко, як і всі високотехнологічні комп'ютерні галузі. У цих умовах забезпечення інформаційної безпеки мереж і систем обробки є пріоритетним завданням для керівництва держави, оскільки від збереження конфіденційності, цілісності й доступності державних інформаційних ресурсів багато в чому залежить якість та оперативність прийняття стратегічних рішень та ефективність їхньої реалізації.

Аналіз останніх досліджень та публікацій. Значний внесок у розвиток теорії та практики побудови кіберпростору і забезпечення його захисту загалом зробили провідні закордонні та вітчизняні науковці такі, як К. Александер, К. Демчак, Лі Джанг, П. Домбровський, Л. Жанчевскі, М. Каветлі, А. Клімбург, Ф. Крамер, Дж. Ліпман, Дж. Ная-мол., Г. Раттрей, С. Старр, Д. Шелдон, О. Адамов, С. Бондаренко, В. Бурячок, В. Бутузов, С. Гнатюк, О. Довгань, Д. Дубов, О. Климчук, О. Корченко, О. Мандзюк, О. Манжай, В. Панченко, В. Петров, В. Пилипчук, О. Потій, М. Присяжнюк, В. Фурашев, В. Хорошко, І. Храбан та інші.

Виділення недосліджених частин загальної проблеми. На сьогодні в роботах вітчизняних та закордонних учених недостатньо уваги приділено вивченню питання структури та складових кіберпростору, а також процесу забезпечення його безпеки.

Мета статті. Метою статті є побудова концептуальної моделі безпеки в межах кіберпростору, що опише складові національної кібербезпеки та дозволить встановити силу зв'язку між відповідними її складовими, а також визначити рівень кібербезпеки.

Виклад основного матеріалу. У проєкті Концепції інформаційної безпеки України [2], зазначено, що інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства й держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Отже, *інформаційна безпека держави* – це комплекс заходів здійснюваних державними органами влади в інформаційній сфері із запобігання порушення цілісності, конфіденційності та доступності інформації, тобто *кібербезпека держави* – система заходів державними органами влади в кіберпросторі, спрямованих на забезпечення стану захищеності державних інформаційних ресурсів.

Виокремлюють три рівні забезпечення інформаційної безпеки:

рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);

державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам) [3].

На підставі раніше викладеного сформулюємо підходи до реалізації захисних заходів щодо забезпечення безпеки інформації у кіберпросторі, що на сьогоднішній день виглядає як трьохетапна модель (рис. 1).

Рис. 1. Трьохетапна модель реалізації захисних заходів щодо забезпечення безпеки інформації в кіберпросторі

Однак наявність відомих підходів до реалізації захисних заходів не вирішує в повному обсязі проблеми ЗІ. Це пов'язано з відсутністю концептуальних моделей захисту, розробка яких на етапах реалізації СЗІ дозволить впроваджувати вищенаведені захисні заходи.

На рис. 2-3 наведено варіанти концептуальних моделей як особи, так і інформаційних ресурсів, які розроблені з урахуванням уже існуючих на сьогодні моделей [1].

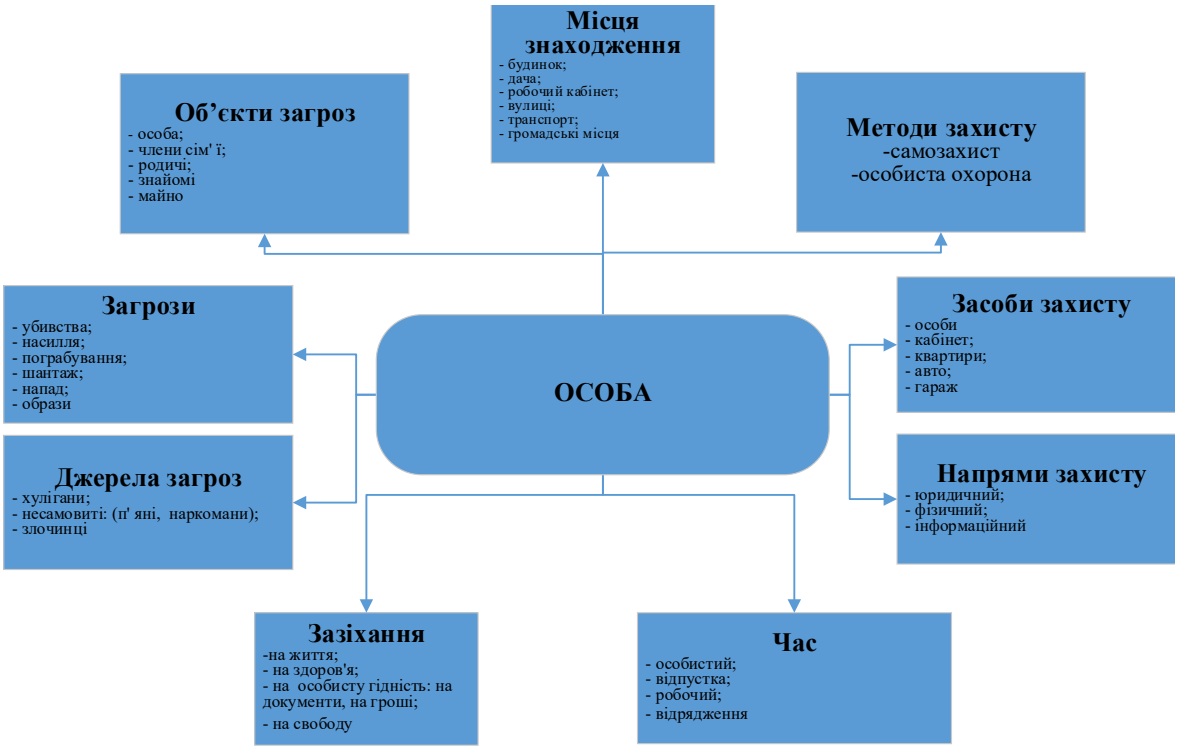

Рис. 2. Концептуальна модель безпеки особи

Рис. 3. Концептуальна модель безпеки інформаційних ресурсів

Важливим з погляду безпеки держави є її нормативно-правове забезпечення. Пропонуємо схематичне представлення концептуальної моделі нормативно-правової безпеки держави (рис. 4).

Рис. 4. Концептуальна модель нормативно-правової безпеки держави

Проаналізувавши концептуальні моделі (рис. 2–4), можна дійти висновку, що їхньою основою є інформація. Отже, можна стверджувати, що при будь-якому розгляді питань керування будь-якою діяльністю центральне місце посідає інформація.

Згідно з Законом України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [5]. Відповідно, інформація тлумачиться як повідомлення про щось, доведення до відома чогось; відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиюсь діяльність.

Інформаційні ресурси в Законі України «Про національну програму інформатизації» [6] визначаються як сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

У Розпорядженні Про схвалення Стратегії розвитку інформаційного суспільства в Україні інформаційні ресурси означаються як систематизована інформація або знання, що мають цінність у певній предметній області й можуть бути використані людиною у своїй діяльності для досягнення певної мети [7].

Під інформаційним ресурсом розуміємо сукупність інформації та її носіїв, інформаційних технологій та інформаційної інфраструктури. Інформаційні ресурси можуть бути поділені на дві групи: державні інформаційні ресурси та недержавні інформаційні ресурси. Недержавні інформаційні ресурси, орієнтовані на пересічного користувача. У своїй роботі ми зосередимо увагу на захисті державних інформаційних ресурсів.

Таким чином, державний інформаційний ресурс є частиною інформаційних ресурсів загалом. Державні інформаційні ресурси – це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства та держави, зафіксовані й систематизовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси, які обробляються і передаються в

інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості та знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку й задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства [9].

До державних інформаційних ресурсів висуваються вимоги щодо актуальності та достовірності наведених у них даних; вичерпної повноти інформаційних джерел; компактності викладу; оперативності пошуку. Державні інформаційні ресурси мають типову структуру: обов'язкову – основну частину і вихідні дані; факультативну – довідково-бібліографічний апарат і додаткову інформацію [4].

Оскільки під суспільним рівнем інформаційної безпеки розуміється формування якісного інформаційно-аналітичного простору, існування незалежних потужних вітчизняних ЗМІ, то в сукупності концептуальна модель безпеки особи та інформаційних ресурсів являтиме собою модель безпеки суспільства (рис. 5). Для наочного представлення даної моделі ми використали діаграми Ейлера-Венна.

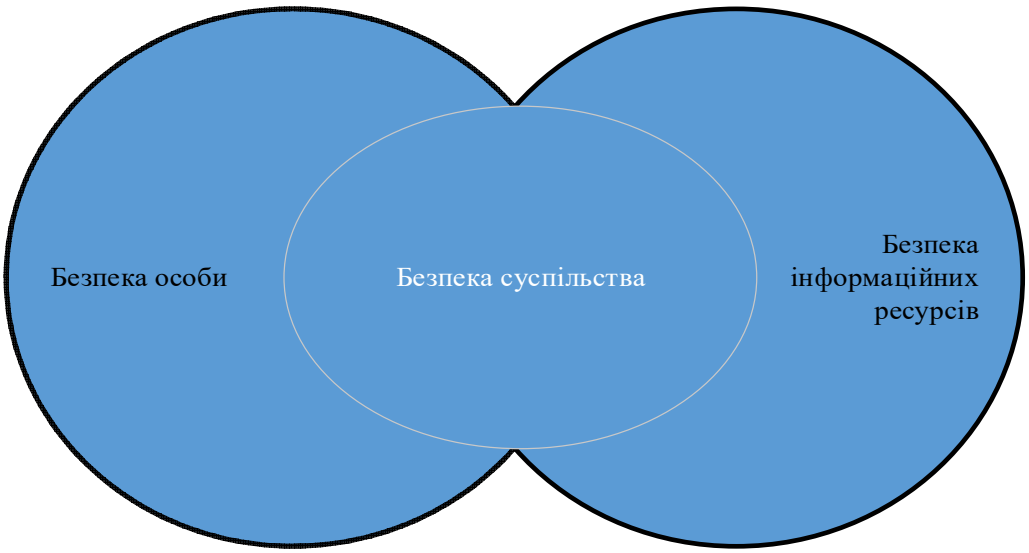

Рис. 5. Концептуальна модель безпеки суспільства

З огляду на вже зібраний і проаналізований фактичний матеріал щодо концептуальних моделей безпеки побудуємо концептуальну модель безпеки держави в межах кіберпростору. Метою її побудови є дослідження кіберпростору держави, визначення його складових та взаємозв'язків між ними та окреслення напрямів покращення його функціонування.

Запропонована нами модель є концептуальною, оскільки їй притаманні характеристики властиві моделям такого виду, зокрема, складається з низки взаємопов'язаних понять, що використовуються для опису кіберпростору держави, поєднує концепцію користувача й розробника моделі, включає в явному виді логіку, обмеження, умови існування. Формалізований опис моделі дає можливість виокремити умови функціонування об'єкта, визначені характером взаємодії між об'єктом і його оточенням, а також між елементами об'єкта керування об'єктом та визначення складу керованих змінних об'єкта.

З погляду забезпечення безпеки в кіберпросторі відповідну концептуальну модель можна представити діаграмами Ейлера-Венна (рис. 6).

Розглянемо на основі теорії множин більш строгий опис такої моделі.

До формування множини елементів моделі безпеки держави в межах кіберпростору (K_i) необхідно залучити експертів із множини $E = \{\bigcup_{j=1}^{n} E_j\} = \{E_1, E_2, \dots, E_n\}$, $E_j \subseteq E (j = \overline{1,n})$, n – кількість експертів, E_j – експерти у сфері кібербезпеки. Ці експерти формують відповідні множини.

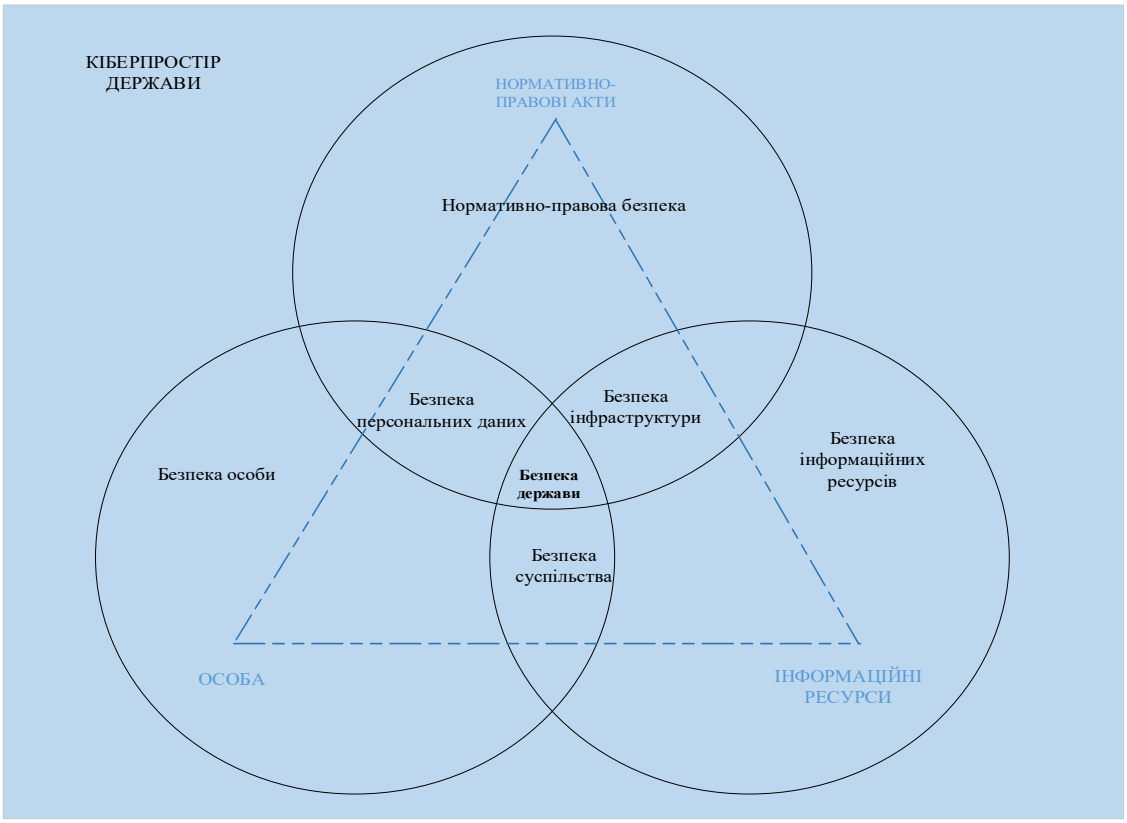

Рис. 6. Концептуальна модель безпеки держави в межах кіберпростору

Множина безпеки особи: $O = \{\bigcup_{k=1}^{m} O_k\} = \{O_1, O_2, \dots, O_m\}$, $O_k \subseteq O (k = \overline{1,m})$, m – кількість елементів, що характеризують множину, O_k – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

Множина безпеки інформаційних ресурсів: $IP = \{\bigcup_{l=1}^{p} IP_l\} = \{IP_1, IP_2, \dots, IP_p\}$, $IP_l \subseteq IP (l = \overline{1,p})$, p – кількість елементів, що характеризують множину, IP_l – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

Множина нормативно-правової безпеки: $NB = \{\bigcup_{f=1}^{z} NB_f\} = \{NB_1, NB_2, \dots, NB_z\}$, $NB_f \subseteq NB (f = \overline{1,z})$, z – кількість елементів, що характеризують множину, NB_f – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

Також згідно з рис. 6 маємо три перерізи по дві множини. Як наслідок, утворюються підмножини, а саме:

- безпека персональних даних: $BP = (O \cap NB) = \{bp | bp \in O \wedge bp \in NB\}$;
- безпека інформаційної структури: $BI = (IP \cap NB) = \{bi | bi \in IP \wedge bi \in NB\}$;
- безпека суспільства: $BS = (O \cap IP) = \{bs | bs \in O \wedge bs \in IP\}$.

Підмножина безпеки персональних даних: $BP = \{\bigcup_{h=1}^{g} BP_h\} = \{BP_1, BP_2, \dots, BP_g\}$, $BP_h \subseteq PB(h = \overline{1,g})$, g – кількість елементів, що характеризують множину, NB_h – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

Підмножина безпеки суспільства: $BS = \{\bigcup_{j=1}^{w} BS_j\} = \{BS_1, BS_2, \dots, SB_w\}, BS_j \subseteq BS(j = \overline{1,w})$, w – кількість елементів, що характеризують множину, BS_j – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

Підмножина безпеки інфраструктури: $BI = \{\bigcup_{u=1}^{q} BI_f\} = \{BI_1, BI_2, \dots, BI_q\}$, $BI_u \subseteq BI(u = \overline{1,q})$, q – кількість елементів, що характеризують множину, BI_f – сформовані експертами у сфері кібербезпеки характеристики елементів множини (можуть описуватись як текстовим повідомленням, так і представлятись у вигляді кількісних показників).

У результати перерізу трьох множин O, IP, NB ми отримаємо множину елементів кібербезпеки держави:

$$D = (O \cap IP \cap NB) = \{d_j | d_j \in O \wedge d_j \in IP \wedge d_j \in NB : j = \overline{1,x} : x = a + b + c\}, \quad (1)$$

де x – кількість елементів множини D, a, b, c – кількість елементів кожної з множини O_k, IP_l, NB_f відповідно, що потрапили до перерізу D.

Формування національної кібербезпеки Т відбувається як об'єднання складових елементів, що входять до моделей безпеки особи, інформаційних ресурсів та нормативно-правової безпеки

$$(T = (O \cup IP \cup NB) = \{t_i | t_i \in O \wedge t_i \in IP \wedge t_i \in NB : i = \overline{1,y} : y = m + p + z - g - q - w + \text{x}\}):$$

$$T = \begin{pmatrix} O_1 & O_2 & \dots & O_k \\ IP_1 & IP_2 & \dots & IP_l \\ NB_1 & NB_2 & \dots & NB_f \end{pmatrix} \quad (2)$$

Оскільки кількість елементів кожної з підмножини O, IP, NB множини T може бути різною, то в цьому випадку треба доповнити рядки до найбільшої розмірності відповідною кількістю, наприклад, одиниць.

Оцінку цінності кожного елемента зазначеної вище множині можна провести за методикою Сааті. Для цього необхідно розглянути скінчену множину елементів альтернатив $D = \{d_1 d_2 \dots d_x\}$. Порівняти довільні два елементи d_s та d_k на предмет встановлення факту, який елемент переважає над іншим та у скільки разів, а потім визначити переваги елементів використовують шкалу відносної важливості об'єктів за Сааті (табл. 1) [8].

Таблиця 1

Шкала відносної важливості об'єктів за Сааті

Визначення	**Ступінь важливості**
об'єкти рівноцінні	1
один об'єкт дещо переважає над іншим	3
один об'єкт краще за інший	5
один об'єкт значно краще за інший	7
один об'єкт абсолютно кращий	9
проміжні судження про об'єкти	2,4,6,8

Експерти за шкалою (див. табл. 1) здійснюють попарні порівняння. У результаті отримаємо матрицю $A = \|a_{ij}\|_{(m \times m)}$, кожний елемент якої a_{ij} являє собою оцінку відносної переваги об'єкта d_s порівняно з елементом d_k $(k, s = \overline{1,x} : x = a + b + c)$.

Припустимо, що $(w_1,\dots,w_m)$ – набір істинних відносних цінностей кожного з елементів множини D. У випадку, якщо відповіді експертів ($a_{ij}=\frac{w_i}{w_j}$) узгоджуються, то справджуються наступні властивості.

Властивість 1. $a_{ij}=1$, $a_{ij}=\frac{1}{a_{ji}}$ для всіх $i,j=\overline{1,m}$, тобто, якщо елемент d_s кращий за d_k у $\alpha>1$ раз, то тоді цінність об'єкта d_k складає $1/\alpha$ цінності об'єкта d_s.

Властивість 2. У випадку повної узгодженості $A=\begin{pmatrix}w_1\\ \dots\\ w_m\end{pmatrix}=m\begin{pmatrix}w_1\\ \dots\\ w_m\end{pmatrix}$.

Вектор $(w_1,\dots,w_m)^T$ є власним вектором матриці A, а m є власним числом цієї матриці.

Далі обчислимо відносні цінності елементів, для яких λ_{max} (де m - найбільше власне число матриці A). Отже, чим ближче λ_{max}, тим краще узгодженими між собою є відповіді експертів. Індекс узгодженості

$$J_p=\frac{\lambda_{\max}}{m-1}. \quad (3)$$

Значення J_p порівнюють з еталонними J_e (табл. 2) [8].

Таблиця 2

Еталонні значення показника узгодженості залежно від кількості об'єктів, що порівнюються

Кількість об'єктів	3	4	5	6	7	8	9	10	11	12	13	14	15
J_e	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,54	1,56	1,57	1,59

Якщо $J_p\le 0{,}1J_e$, то результати опитування експертів задовільні.

Обчислення показника відносної цінності елементів здійснюється для кожного рядка матриці A за формулою:

$$w_i=\frac{\sqrt[m]{a_{11}\dots a_{im}}}{\sum_{i=1}^{m}\sqrt{a_{i1}\dots a_{im}}},\ i=\overline{1,m}. \quad (4)$$

Останнім кроком є аналіз експертами отриманих результатів та прийняття рішень.

Важливим елементом для нашої моделі є встановлення сили зв'язку між відповідними множинами та їх елементами та прогнозування можливих впливів на кібербезпеку держави. Для цього необхідно розрахувати коефіцієнт кореляції та побудувати регресійне рівняння.

Лінійний коефіцієнт парної кореляції r_{xy} досліджує щільність зв'язку між явищ, що вивчаються ($-1\le r_{xy}\le 1$):

$$r_{xy}=\frac{\frac{1}{n}\sum_i(x_i-\overline{x})(y_i-\overline{y})}{\sigma_x\sigma_y}=\frac{\overline{yx}-\overline{y}\cdot\overline{x}}{\sqrt{(\overline{x^2}-\overline{x}^2)\cdot(\overline{y^2}-\overline{y}^2)}} \quad (5)$$

Коефіцієнт кореляції має такі *властивості*:

він набуває значення на відрізку [–1; 1], тобто $-1\le r\le 1$. Чим ближче $|r|$ до 1, тим тісніше кореляційний зв'язок;

при $|r|=1$ кореляційний зв'язок стає функціональним. При цьому всі спостережувані значення лежать на одній лінії;

при $r=0$ кореляційний зв'язок відсутній та лінія регресії паралельна осі *x*.

При $r>0$ ($b_1>0$) кореляційний зв'язок називається *прямим*, а при $r<0$ ($b_1<0$) кореляційний зв'язок називається *зворотним*. У результаті отримаємо матрицю коефіцієнтів парної кореляції:

$$R = \begin{pmatrix} 1 & r_{y1} & r_{y2} & \dots & r_{yk} \\ r_{1y} & 1 & r_{12} & \dots & r_{1k} \\ r_{2y} & r_{k2} & 1 & \dots & r_{2k} \\ \dots & \dots & \dots & \dots & \dots \\ r_{ky} & r_{k1} & r_{k2} & \dots & 1 \end{pmatrix} \quad (6)$$

Ця матриця є симетричною, тобто коефіцієнти кореляції між результуючою змінною y – *безпекою держави* та факторною ознакою x_j – *елементи перерізу D* рівні між собою ($r_{yj} = r_{jy}$, $j = \overline{1,k}$), коефіцієнти кореляції між i-м та j-м факторами теж рівні ($r_{ij} = r_{ji}$, $i = \overline{1,k}, j = \overline{1,k}$).

Якщо значення коефіцієнта парної кореляції між факторами наближене до одиниці, то це свідчить про тісний зв'язок між ними. У цьому випадку один із факторів необхідно вилучити з розгляду, тобто не враховувати під час побудови рівняння регресії (бажано залишити фактор, який є вагомішим з погляду експертів або той, що сильніше корелює з результуючою змінною y).

Оскільки на безпеку держави впливають багато факторів, то у цьому випадку маємо справу з множинною (багатофакторною) лінійною моделлю (регресією), що описує взаємний зв'язок між залежною змінною y (*безпека держави) та факторами* $x_1, x_2, \dots, x_m$ (*елементи перерізу D*) і яку можна подати у такому вигляді: $y = f(x_1, x_2, x_3 \dots x_m, \varepsilon)$, де y - залежна (результуюча) змінна; x_j, $(j = \overline{1,m})$ - незалежні змінні; ε - стохастична складова.

Аналітична форма цієї моделі може бути різною залежно від сутності зв'язків. Найбільш поширена форма залежності – лінійна: $Y = b_0 + b_1 \cdot x_i + e_i$, де b_0 – вільний член, який визначає значення y_i за умови, коли значення факторів дорівнюють нулеві; x_{ij} $(i = \overline{1,n}, j = \overline{1,m})$ – значення X_j-го фактору при *i*-му спостереженні; b_j $(j = \overline{1,m})$ – теоретичні коефіцієнти регресії (часткові коефіцієнти) або параметри теоретичної регресії, які характеризують реакцію залежної змінної y_i $(i = \overline{1,n})$ на зміну кожного фактора X_j $(j = \overline{1,m})$; ε_i – випадковий збудник при *i*-му спостереженні.

Для однозначного визначення параметрів b_j моделі необхідно, щоб виконувалась нерівність $n \geq m + 1$, де *n* – число спостережень; *m* – число факторів у моделі.

У векторно-матричній формі теоретичну модель можна подати так:

$$\vec{Y} = X \cdot \vec{A} + \vec{\varepsilon}, \text{ де}$$

$$\vec{Y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_i \\ \vdots \\ y_n \end{pmatrix}, X = \begin{pmatrix} 1 & x_{11} & \dots & x_{1j} & \dots & x_{1m} \\ 1 & x_{21} & \dots & x_{2j} & \dots & x_{2m} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & x_{i1} & \dots & x_{ij} & \dots & x_{im} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & x_{n1} & \dots & x_{nj} & \dots & x_{nm} \end{pmatrix}, \vec{A} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_j \\ \vdots \\ b_m \end{pmatrix}, \vec{\varepsilon} = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_i \\ \vdots \\ \varepsilon_n \end{pmatrix}. \quad (7)$$

Іншими формами залежності можуть бути:

1) $Y = b_0 + b_1 X$ – лінійна;

2) $Y = b_0 X^{b_1}$ – степенева;

3) $Y = b_0 \cdot b_1^X$ – показникова;

4) $Y = b_0 + \frac{b_1}{X}$ – гіперболічна та інші, де b_0, b_1 – невідомі параметри моделі.

Неважко переконатись, що наведені нелінійні форми залежності за допомогою елементарних перетворень приводяться до лінійних.

Зауважимо, що між факторними ознаками може виникнути явище мультиколінеарності, тобто висока залежність (корельованість) різних факторів.

Для виявлення мультиколінеарності можна використати критерій (алгоритм) Феррара-Глобера. Цей алгоритм має три види статистичних критеріїв, згідно з якими перевіряється мультиколінеарність усього масиву незалежних змінних (χ^2 – «хі»-квадрат); кожної незалежної змінної з рештою змінних (*F*-критерій); кожної пари незалежних змінних (*t*-критерій).

При наявності мультиколінеарності факторів доцільно звернути увагу і на специфікацію моделі. Іноді заміна однієї функції іншою, не суперечить інформації, дозволяє усунути мультиколінеарність.

У випадку моделей з великою кількістю факторів, коли не вдається позбутися мультиколінеарності, параметри моделі оцінюють не методом найменших квадратів, а методом головних компонент.

Оскільки факторні ознаки, які включаються в модель, можуть бути в різних одиниця вимірювання, то необхідно проводити *стандартизацію (нормалізацію) змінних.* Елементи стандартизованих векторів розрахуємо за формулою:

$$X_{ik}^{*} = \frac{X_{ik} - \overline{X}_k}{\sqrt{n\sigma^2_{X_k}}}, \tag{8}$$

де *n* – число спостережень, *m* – число незалежних змінних, $i=\overline{1,n}$, $k=\overline{1,m}$, $\overline{X_k}$ – середня арифметична *k*-ї незалежної змінної, $\sigma^2_{X_k}$ – дисперсія *k*-ї незалежної змінної.

Перш ніж визначити істинні значення параметрів, ми можемо визначити рівень національної кібербезпеки, а саме, якщо отримане значення результуючої $y = f(x_1, x_2, x_3, ..., x_m, \varepsilon)$, знаходиться в межах від 0 до 1, чим ближче до 1, тим рівень безпеки вище. При цьому будемо вважати, що 0-0,3 рівень безпеки *неприйнятний*; 0,3-0,7– *низький*; 0,7-1 – *достатній*.

Істинні оцінки параметрів моделі визначаються за формулами:

$$b_1 = b_1^* \times \left(\frac{\sigma_Y}{\sigma_{X_1}}\right), b_2 = b_2^* \times \left(\frac{\sigma_Y}{\sigma_{X_2}}\right), b_3 = b_3^* \times \left(\frac{\sigma_Y}{\sigma_{X_3}}\right), \ldots, b_n = b_n^* \times \left(\frac{\sigma_Y}{\sigma_{Xn}}\right) \tag{9}$$

$$b_0 = \bar{Y} - b_1\bar{X}_1 - b_2\bar{X}_2 - b_3\bar{X}_3 + \ldots + b_n\bar{X}_n.$$

Обов'язковим є перевірка множинної лінійної моделі на точність (якість). Загальну якість рівняння регресії оцінюють через розрахунок *коефіцієнта детермінації.*

Коефіцієнт детермінації показує, яка частина зміни залежної змінної обумовлена зміною незалежного фактору ($0 \le R^2 \le 1$). Чим ближче R^2 до 1, тим краще рівняння регресії наближає (апроксимує) експериментальні дані. У випадку парної регресії $R^2 = r^2$, де r – коефіцієнт кореляції. Коефіцієнт детермінації обчислюється за формулою:

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{y}_i - \bar{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2} = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}. \tag{10}$$

Середня похибка апроксимації – середнє відносне відхилення розрахункових значень від фактичних:

$$\overline{A} = \frac{1}{n}\sum\left|\frac{y_i - \hat{y}_i}{y_i}\right| \cdot 100\ \%. \tag{11}$$

Побудоване рівняння регресії вважається задовільним, якщо значення $\overline{A}$ не перевищує 10-12 %.

Чим вищій показник детермінації або чим менша середня похибка апроксимації, тим краще побудована модель описує вихідні дані.

Оцінка значущості всього рівняння регресії загалом здійснюється за допомогою *F*-критерію Фішера. *F*-критерій Фішера полягає в тому, що проводиться перевірка гіпотези H_0 про статистичну значущість рівняння регресії. Для цього виконується порівняння фактичного $F_{\text{факт}}$ та табличного (критичного) $F_{\text{табл}}$ значень *F*-критерію Фішера. $F_{\text{факт}}$ визначається за формулою:

$$F_{\text{факт}} = \frac{\sum\frac{(\hat{y}_i-\overline{y})^2}{m}}{\sum\frac{(y_i-\hat{y}_i)^2}{n-m-1}} = \frac{r_{xy}^2}{1-r_{xy}^2} \cdot \frac{n-m-1}{m}, \quad (12)$$

де n – кількість одиниць сукупності, m – кількість параметрів при змінних (для лінійної регресії m = 1). Для нелінійної регресії замість r_{xy}^2 використовують R^2.

$F_{\text{табл}}$ – максимально можливе значення критерію під впливом випадкових факторів при ступенях вільності $k_1 = m$, $k_2 = n$-m-1 та рівні значущості α. Рівень значущості α – ймовірність відкинути правильну гіпотезу при умові, що вона є вірна. Зазвичай α надають значення 0,05 або 0,01. Це означає, що у 5 або 1 % випадків ми можемо помилитися, а у 95 або 99 % випадків (рівень довіри) наші висновки будуть правильними.

Якщо $F_{\text{табл}} < F_{\text{факт}}$, то гіпотеза H_0 відхиляється та визнається статистична значущість та надійність рівняння регресії.

Якщо $F_{\text{табл}} > F_{\text{факт}}$, то гіпотеза H_0 не відхиляється та визнається статистична незначущість та ненадійність рівняння регресії.

Для оцінки статистичної значущості коефіцієнтів лінійної регресії та лінійного коефіцієнта парної кореляції r_{xy} застосовують також *t*-критерій Стьюдента та розраховують довірчі інтервали кожного з показників. *t*-критерій Стьюдента полягає в тому, що висувається гіпотеза H_0 про випадкову природу показників, тобто про незначне їх відхилення від нуля. Фактичне значення критерію $t_{\text{факт}}$ для коефіцієнтів регресії та коефіцієнта кореляції r_{xy} розраховується шляхом порівняння їхніх значень із величиною стандартної похибки:

$$t_{b_0} = \frac{b_0}{m_{b_b}}; t_{b_1} = \frac{b_1}{m_{b_1}}; t_r = \frac{r_{xy}}{m_{r_{xy}}}. \quad (13)$$

Стандартні похибки обчислюється за формулами:

$$m_{b_1} = \sqrt{\frac{\frac{\sum(y_i-\hat{y}_i)^2}{n-2}}{\sum(x_i-\overline{x})^2}}; m_{b_0} = \sqrt{\frac{\sum(y_i-\hat{y}_i)^2}{n-2} \cdot \frac{\sum {x_i}^2}{n\sum(x_i-\overline{x})^2}}; m_{r_{xy}} = \sqrt{\frac{1-r_{xy}^2}{n-2}}. \quad (14)$$

Порівнюючи фактичне та табличне значення для *t*-критерію роблять відповідні висновки.

$t_{табл}$ - максимально можливе значення критерію під впливом випадкових факторів для $k = n$-2 ступенів вільності та рівні значущості α.

Якщо $t_{\text{табл}} < t_{\text{факт}}$, то гіпотеза H_0 відхиляється (тобто коефіцієнти рівняння регресії та коефіцієнт кореляції r_{xy} не випадково відмінні від нуля та сформовані під впливом систематично діючого фактору x).

Якщо $t_{\text{табл}} > t_{\text{факт}}$, то гіпотеза H_0 не відхиляється та визнається випадкова природа формування b_0, b_1 та r_{xy}.

Довірчі інтервали

Довірчі інтервали визначають межі, в яких лежать точні значення визначених показників, із заданим ступенем достовірності.

Для розрахунку довірчих інтервалів для параметрів b_0 та b_1 рівняння лінійної регресії визначають граничну похибку Δдля кожного показника:

$$\Delta_{b_0} = t_{\text{табл}} \cdot m_{b_0}; \Delta_{b_1} = t_{\text{табл}} \cdot m_{b_1}. \quad (15)$$

де *$t_{табл}$* – це табличне значення t-критерію Стьюдента для $k = n - 2$ ступенів вільності та заданого рівня значущості α.

Тоді довірчі інтервали обчислюються:

$$\gamma_{b_0} = b_0 \pm \Delta_{b_0}; \gamma_{b_1} = b_1 \pm \Delta_{b_1}. \quad (16)$$

Якщо в межі довірчого інтервалу потрапляє нуль (тобто нижня границя від'ємна, а верхня – додатна), то параметр, що оцінюється приймається за нуль.

Висновки відповідно до статті. Отже, у загальному вигляді концептуальна модель безпеки кіберпростору формується на основі трьох компонентів: *особи*, яка обробляє інформацію, володіє нею або здійснює її захист; *нормативно-правові акти*, які забезпечують юридичний захист інформації; *інформаційні ресурси*, у яких сконцентровано інформацію, що потребує захисту, і в межах яких функціонують засоби захисту інформації.

Список використаних джерел

1. Концептуальные вопросы защиты информации. URL: https://www.google.com/search?q=%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F+%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C+%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B+%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8&rlz=1C1SQJL_enUA890UA890&sxsrf=ALeKk03qyNTXuFj6XQwdUCKQmanlrQwEWw:1589031719240&tbm=isch&source=iu&ictx=1&fir=qVMgT6wY08z3yM%253A%252CAYMUdVgt__OzKM%252C_&vet=1&usg=AI4_-kR42qyP1rSdiJfxnasMXu26g6SjRg&sa=X&ved=2ahUKEwj10aW59KbpAhXBo4sKHWzdBp8Q9QEwAHoECAkQAw#imgrc=2Ljpf2cnn3HIkM.

2. Концепція інформаційної безпеки України : проєкт. URL: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20(%D0%A2%D0%B5%D0%BA%D1%81%D1%82)%20-%2030.09.15.pdf.

3. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. *Часопис Київського університету права*. 2010. № 4. С. 317–321.

4. Приймак Ю. Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг. *Державне управління: теорія та практика*. 2009. № 2. URL: www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf.

5. Про інформацію : Закон України від 2жовтня 1992 року № 2658-XII. URL: http://zakon3.rada.gov.ua/ laws/show/2657-12/ed20110106.

6. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР. *Відомості Верховної Ради України*. 1998. № 27-28. С. 181.

7. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України; Стратегія від 15.05.2013 № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21.

8. Скітер І. С., Ткаленко Н. В., Трунова О. В. Математичні методи прийняття управлінських рішень. Чернігів : ЧДІЕУ, 2011. 247 с.

9. Юдін О. К., Бучик С. С. Концептуальний аналіз уразливості державних інформаційних ресурсів. *Наукоємні технології. Технічні науки*. 2013. № 3(19). С. 299–304.

References

1. Conceptual issues of information security. https://www.google.com/search?q=%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F+%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C+%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B+%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8&rlz=1C1SQJL_enUA890UA890&sxsrf=ALeKk03qyNTXuFj6XQwdUCKQmanlrQwEWw:1589031719240&tbm=isch&source=iu&ictx=1&fir=qVMgT6wY08z3yM%253A%252CAYMUdVgt__OzKM%252C_&vet=1&usg=AI4_-kR42qyP1rSdiJfxnasMXu26g6SjRg&sa=X&ved=2ahUKEwj10aW59KbpAhXBo4sKHWzdBp8Q9QEwAHoECAkQAw#imgrc=2Ljpf2cnn3HIkM.

2. The concept of information security of Ukraine: project. http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20(%D0%A2%D0%B5%D0%BA%D1%81%D1%82)%20-%2030.09.15.pdf.

3. Kuzmenko, A. M. (2010). Osoblyvosti problem zakonodavchoho zabezpechennia informatsiinoi bezpeky derzhavy, suspilstva i hromadianyna v umovakh informatsiino-psykholohichnoho protyborstva [Features of problems of legislative maintenance of information security of the state, society and the citizen in the conditions of information and psychological confrontation]. *Chasopys Kyivskoho universytetu prava – Journal of Kyiv University of Law,* 4, pp. 317–321.

4. Pryimak, Yu. Iu. (2009). Natsionalni informatsiini resursy – dzherelo derzhavnykh informatsiinykh produktiv ta posluh [National information resources are a source of state information products and services]. *Derzhavne upravlinnia: teoriia ta praktyka – Public administration: theory and practice*, (2). www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf.

5. Pro informatsiiu [On Information], Law of Ukraine № 2658-XII (October 2, 1992). http://zakon3.rada.gov.ua/ laws/show/2657-12/ed20110106.

6. Pro Natsionalnu prohramu informatyzatsii [On the National Informatization Program], Law of Ukraine № 74/98-BP (on February 4, 1998). *Information of the Verkhovna Rada of Ukraine,* (27-28), p. 181.

7. Pro skhvalennia Stratehii rozvytku informatsiinoho suspilstva v Ukraini [On approval of the Information Society Development Strategy in Ukraine], Order of the Cabinet of Ministers of Ukraine; Strategy № 386-p (May 15, 2013). https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21.

8. Skiter, I. S., Tkalenko, N. V., Trunova, O. V. (2011). *Matematychni metody pryiniattia upravlinskykh rishen [Mathematical methods of managerial decision making]*. ChDIEU.

9. Yudin, O. K., Buchyk, S. S. (2013). Kontseptualnyi analiz urazlyvosti derzhavnykh informatsiinykh resursiv [Conceptual analysis of vulnerability of state information resources]. *Naukoiemni tekhnolohii – Science-intensive technologies. Technical sciences,* (3(19)), pp. 299–304.

UDC 004.056:351.861

Yuliia Tkach

CONCEPTUAL MODEL OF CYBER SPACE SECURITY

Urgency of the research. *Public information resources and means of electronic network transactions (servers, routers, remote access servers, communication channels, operating systems, databases and applications) must be protected reliably and efficiently: the price of each "break" of protection is growing rapidly and this growth will continue in the near future.*

Target setting. *Ensuring information security of networks and processing systems is a priority for the state leadership, as the quality and efficiency of strategic decision-making and the effectiveness of their implementation largely depend on maintaining the confidentiality, integrity and availability of state information resources.*

Actual scientific researches and issues analysis. *Despite the ever-increasing number of publications on information security, the problem of security in cyberspace, especially a state one, remains unresolved.*

Uninvestigated parts of general matters defining. *Currently, in the works of domestic and foreign scientists, insufficient attention is paid to the development of systems and models of cybersecurity of the state.*

The research objective. *The aim of the article is to build a conceptual model of security within cyberspace, which will describe the components of national cybersecurity and will establish the strength of the connection between its relevant components, as well as determine the level of cybersecurity.*

The statement of basic materials. *Using Euler-Venn diagrams, the cyberspace of the state is graphically represented and a more rigorous description of the model is proposed on the basis of set theory. In general, the conceptual model of cybersecurity is formed on the basis of three components: a person who processes information, owns it or protects it; regulations that provide legal protection of information; information resources, where the information in need of protection is concentrated, and within which means of information protection function.*

Conclusions. *The article builds a conceptual model of state security, which describes the components of cybersecurity of the state and allows to establish the strength of the connection between its relevant components, as well as to determine the level of cybersecurity.*

Keywords: *cyberspace; conceptual model; information security of the state; information security.*

Fig.: 6. Table: 2. References: 9.

Ткач Юлія Миколаївна – доктор педагогічних наук, професор, завкафедри кібербезпеки та математичного моделювання, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yuliia – Doctor of Pedagogical Science, Professor, Head of Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: https://orcid.org/0000-0002-8565-0525
SCOPUS Author ID: 57193026076