УДК 004.056

СТРАТЕГІЯ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ДЕРЖАВИ ВІД РИЗИКУ СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ

Володимир Бурячок, Олександр Корченко, Володимир Хорошко, Вадим Кудінов

У промислово розвинутих країнах завдання оцінювання рівня захищеності їх інформаційної і кіберінфраструктури від ризику стороннього кібернетичного впливу належить до низки пріоритетних. Його вирішення нині неможливе без комплексного дослідження спроможності систем кібернетичної безпеки цих країн протидіяти такому впливу та його деструктивним наслідкам. Передусім це обумовлюється безперервним зростанням обсягу інформації, що циркулює, накопичується і обробляється в інформаційних і кіберпросторах цих країн, збільшенням швидкостей її передачі, бурхливим розвитком нових інформаційно-телекомунікаційних технологій і загальною комп'ютеризацією, зокрема доступом до всесвітньої мережі Інтернет, а також необхідністю захисту такої інформації від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз. З урахуванням цього викладено стратегію дій, яка дасть можливість: по-перше – оцінити рівень захищеності інфосфери держави від ризику стороннього кібервпливу; по-друге – одержати кількісне значення "індексу кіберпотужності", що характеризує готовність державних об'єктів інформаційної і кіберінфраструктури до безпечного функціонування за таких умов; по-третє – встановити вимоги до формування державної системи кібернетичної безпеки та розробити заходи спрямовані на підвищення її результативності. Встановлено, що на ступінь критичності кібербезпеки до атак у кіберпросторі головним чином впливає наявність сформованої і чітко функціонуючої нормативно-правової бази та розгалуженої технологічної інфраструктури країни, стан її соціально-економічного розвитку, а також ступінь використання країною інформаційно-комунікаційних технологій та систем. Для оцінювання рівня захищеності запропоновано використовувати метод анкетування – один із відомих методів експертного оцінювання.

***Ключові слова**: стратегія оцінювання, оцінювання рівня захищеності, кібернетичний вплив, інформаційно-комунікаційна технологія, кібербезпека, кіберзагроза, кіберпростір.*

Постановка завдання у загальному вигляді. Наприкінці XX – початку XXI сторіччя завдяки глибоким системним перетворенням, викликаним синтезом перспективних інформаційно-комунікаційних технологій (ІКТ) та бурхливим розвитком інформаційно-телекомунікаційних (ІТ) систем і мереж почали формуватись принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний і кіберпростори. Поступово вони накопичили практично необмежений потенціал й нині, за рахунок забезпечення оброблення і передавання їх головного об'єкта – інформації, відіграють суттєву роль в економічному і соціальному розвитку переважної більшості країн світу. Безперервне збільшення обсягів і швидкостей передачі інформації та загальна комп'ютеризація, зокрема доступ до всесвітньої мережі Інтернет, у свою чергу привели до необхідності: регулювання систем національної безпеки цих країн; формування цими країнами стратегічних і поточних завдань внутрішньої й зовнішньої політики щодо забезпечення власної інформаційної і кібернетичної безпеки (кібербезпеки).

З огляду на те, що одна із складових національних інтересів України в інфосфері містить у собі розвиток вітчизняної індустрії інформації, в тому числі індустрії засобів інформатизації, телекомунікації та зв'язку, неправомірний обіг з якими може завдати шкоди їхньому власникові, користувачеві або іншій особі – оцінювання рівня захищеності окремих об'єктів державної інформаційної і кіберінфраструктури, а також національної інфосфери в цілому від ризику стороннього кібернетичного впливу (кібервпливу) є завданням першочерговим й до того ж таким, що має практичне значення.

Аналіз останніх досліджень і публікацій. Зазначене завдання в певних аспектах висвітлено у публікаціях як зарубіжних, так і вітчизняних авторів. Найвідомішими серед них є роботи А.В. Возженікова, В.І. Ярочкіна, Г. Почепцова, М. Лібіцкі, К.А. Мініхена, О. Шермана, Ф. Фукуями та інших фахівців. Проте аналіз цих та багатьох інших джерел свідчить, що комплексного оцінювання більшістю держав світу власного рівня захищеності від ризику стороннього кібернетичного впливу в цілому, а також окремих об'єктів їх інформаційної і кіберінфраструктур до цього часу нажаль не проводилось. Тому воно потребує додаткового і більш глибокого вивчення.

Актуальність та мета статті. Отже, актуальність статті зумовлено передусім обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає, а також потребою підвищення результативності захисту інфосфери України від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз.

Метою статті є оцінювання готовності окремих об'єктів інформаційної і кіберінфраструктури нашої держави, а також її інфосфери в цілому до безпечного функціонування в умовах стороннього кібернетичного впливу та встановлення на підставі фактору "індексу кіберпотужності" вимог до відповідних систем кібернетичної безпеки.

Виклад основного матеріалу. Завдання на кшталт оцінювання рівня захищеності країн світу від ризику стороннього кібернетичного впливу відносяться, як відомо, до класу багатокритеріальних. Для їх колегіального рішення в умовах невизначеності і конфлікту серед існуючих методів математичного моделювання, методів формування та дослідження узагальнених показників якості з використанням графоаналітичного і ним подібних підходів, експертних методів вирішення складних завдань оцінювання та вибору будь-яких об'єктів, в тому числі спеціального призначення, а також аналізу та прогнозування ситуацій з великою кількістю значимих факторів, найбільш раціональними і визначальними є саме експертні методи. Вони дають можливість більш глибоко вивчити явища, які істотно впливають на рівень захищеності як держави в цілому, так і окремих об'єктів її інформаційної та кіберінфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз, виявити найбільш важливе та істотне у цих процесах, не опускаючи тих деталей і взаємозв'язків, без яких не може бути побудована модель досліджуваної ситуації. Підвищенню ефективності застосування експертних методів як правило сприяє:

- проведення обґрунтованого добору групи висококваліфікованих експертів, діяльність яких пов'язана з проведенням досліджень за обраними для проведення експертизи напрямами й посади яких відповідають вимогам до таких у обраній галузі знань;
- своєчасне ознайомлення експертів з метою дослідження та пояснення їм змісту роботи, яку вони повинні виконати;
- проведення процедури анкетування експертів з урахуванням усіх особливостей конкретного завдання;
- проведення експертизи кожного заходу із забезпечення кібербезпеки держави або окремих об'єктів її інфраструктури відносно визначених вимог за встановленими індикаторами та відповідними їм показниками.

Враховуючи таке останнім часом значного поширення серед відомих методів експертного оцінювання, що дозволяють безпосередньо використовувати судження та інтуїцію експертів у будь-якій формалізованій структурі [1] для вирішення завдань з соціальним, політичним або воєнним змістом отримав метод анкетування.

Першим кроком методу є визначення предметної галузі експертизи та формування завдання групам експертів на її проведення.

Другим кроком – формування структури бази знань з предметної галузі експертизи. Сформовані групи експертів: аналізують список індикаторів, які визначають суть кібербезпеки за певними категоріями; перевіряють повноту списку показників, які відображають бажаний рівень кібербезпеки за кожним з індикаторів та здійснюють довизначення значень індикаторів і показників у випадку неповноти вихідного списку; визначають проміжну мету дослідження – ранжирування показників; перевіряють відповідність обраного математичного метода задачі, яку необхідно вирішити.

Третім кроком методу є проведення розрахунку компетентності сформованої групи експертів в ході вирішення глобальної мети дослідження. При цьому оцінювання компетентності експертів здійснюється одним із відомих методів самооцінки і взаємного оцінювання, або ж на підставі їх інтуїції. В подальшому обчислюються узагальнені оцінки компетентності, які використовуються як вагові коефіцієнти висловлювань експертів. Експерт, який отримає максимальний коефіцієнт компетентності виділяється як Головний експерт, уповноважений приймати рішення. На нього покладається прийняття рішення відносно ступеня критичності кіберзагроз для безпеки країни.

На четвертому кроці визначається показник комплексної оцінки рівня захищеності держави від ризику стороннього кібернетичного впливу.

На п'ятому – відбувається документування та аналіз результатів експертизи.

Таким чином, застосування даної стратегії дасть можливість Головному експерту одержати числову характеристику комплексного показника оцінки рівня захищеності держави від впливу внутрішніх і зовнішніх кібернетичних втручань і загроз та прийняти рішення про його відповідність заданим вимогам. При цьому під:

- *по-перше*, кібербезпекою будемо розуміти стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу;
- *по-друге*, стороннім кібервпливом – деструктивні дії, що в процесі інформаційного протиборст-

ва зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційного ресурсу (ІР), ІКТ та ІТС й здійснюються ними шляхом: поширення вірусного програмного забезпечення (ПЗ); застосування апаратних закладок; використання несертифікованого ПЗ та засобів захисту інформації; радіоелектронного та іншого впливу на технічні і програмні засоби, а також системи телекомунікацій та зв'язку; несанкціонованого доступу до відносно відкритих і закритих електронних джерел та інформаційних мереж;проведення кібернетичних атак тощо;

– *по-третє*, об'єктами інформаційної і кіберінфраструктури – ІР та ІКТ, а також ІТ системи та мережі усіх форм власності, що керуються автоматизованими системами управління й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протиборчої сторони.

Розкриємо суть запропонованої методики з точки зору одного експерту. Індекс кіберпотужності у цьому випадку вважатимемо динамічною кількісно-якісною характеристикою, яка вказує на здатність держав забезпечити власну кібербезпеку та підтримувати безпечне функціонування об'єктів їх інформаційної і кіберінфраструктури в умовах кіберзагроз. Його визначення здійснюється на підставі виявлення відхилень від штатного режиму функціонування ІР, ІТ систем і мереж, а також програмних і апаратних засобів шляхом аналізу чотирьох основних категорій, а саме:

1) наявної нормативно-правової бази;

2) стану соціально-економічного розвитку держави;

3) наявності розгалуженої технологічної інфраструктури;

4) ступеня використання ІКТ та ІТС у розвитку інформаційного суспільства.

Кожна з цих категорій включає низку узагальнених індикаторів таких, як:

1.1) ставлення керівництва держави до питань забезпечення кібербезпеки:

– наявність національної стратегії (доктрини тощо) з кібербезпеки; наявність нормативно-законодавчого забезпечення сфери кібербезпеки;

– наявність міжнародних зобов'язань країни у сфері кібербезпеки;

– наявність співробітництва державних і приватних структур у сфері кібернетичної безпеки;

1.2) стан розвитку політики кіберзахисту:

– рівень діяльності керівництва держави у питаннях кіберзахисту;

– рівень діяльності суб'єктів інформаційної і кіберінфраструктури у питаннях кіберзахисту;

2.1) рівень освіти, науки та техніки:

– частка населення з вищою освітою;

– частка населення, що володіє іноземною й передусім англійською мовою;

– частка НДР та ДКР з питань кібербезпеки;

– рівень залучення до виконання НДДКР інженерно-технічного персоналу;

2.2) рівень розвитку інноваційного середовища:

– стан витрат на проведення НДДКР;

– стан патентно-раціоналізаторської роботи (кількість патентів);

– стан залучення приватного та венчурного капіталу;

3.1) якісний стан технологічної інфраструктури:

– рівень використання Інтернет (у т.ч. поширення Wi-Fi – точок доступу);

– рівень використання засобів мобільного зв'язку та соціальних мереж;

3.2) рівень впровадження технологічної інфраструктури:

– рівень фінансування заходів з впровадження ІКТ (у відношенні до ВВП);

– рівень безпеки сервісів;

4.1) використання ІКТ у:

– корпоративних мережах;

– інтелектуальних транспортних системах;

4.2) використання ресурсів мережі Інтернет для:

– розміщення пропозицій щодо надання товарів і послуг;

– замовлення товарів і послуг.

На основі наведених вище індикаторів, що характеризують здатність країни забезпечити кібербезпеку і підтримувати безпечне функціонування власних об'єктів інформаційної і кіберінфраструктури, розробимо ієрархічну схему їх показників (табл. 1) в якій значення попереднього -го рівня визначаються значенням відповідних показників $(i+1)$-го рівня [2]. При цьому категоріям поставлена у відповідність сукупність специфічних індикаторів, що в свою чергу описані елементарними характеристиками, які отримали назву показників.

Кожній категорії 2-го рівня, кожному індикатору 3-го рівня та кожному показнику 4-го рівня ієрархії за певним правилом, наприклад шляхом експертного опитування [2], може бути поставлене у відповідність деяке число (табл. 2, табл. 4). Обов'язковою умовою при цьому є наступне: сума ваг категорій, індикаторів та показників одного рівня завжди має дорівнювати одиниці.

Ієрархічна схема рівня критичності кібербезпеки Таблиця 1

Рівень критичності кібербезпеки								1-й рівень
НАЯВНІСТЬ НОРМАТИВНО-ПРАВОВОЇ БАЗИ		**СТАН СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ ДЕРЖАВИ**		**НАЯВНІСТЬ РОЗГАЛУЖЕНОЇ ТЕХНОЛОГІЧНОЇ ІНФРАСТРУКТУРИ**		**СТУПІНЬ ВИКОРИСТАННЯ ІКТ ТА ІТС**		2-й рівень (категорії)
Ставлення керівництва держави до питань забезпечення кібербезпеки	Стан розвитку політики кіберзахисту	Рівень освіти, науки та техніки	Рівень розвитку інноваційного середовища	Якісний стан технологічної інфраструктури	Рівень впровадження технологічної інфраструктури	Використання інформаційно-комунікаційних технологій у ЛОМ	Використання ресурсів мережі Інтернет у комерційній діяльності	3-й рівень (індикатори)
$A1_1$, $A1_2$, $A1_3$, $A1_4$	$A2_1, A2_2$	$B1_1, B1_2$, $B1_3, B1_4$	$B2_1, B2_2$, $B2_3$	$C1_1, C1_2$	$C2_1, C2_2$	$D1_1, D1_2$	$D2_1, D2_2$	4-й рівень (показники)

Значення вагових коефіцієнтів категорій і індикаторів рівня критичності кібербезпеки Таблиця 2

Позначення категорій та індикаторів рівня критичності	Позначення вагових коефіцієнтів категорій та індикаторів	Значення вагових коефіцієнтів категорій та індикаторів	Сума вагових коефіцієнтів індикаторів
<**НАЯВНІСТЬ НОРМАТИВНО-ПРАВОВОЇ БАЗИ**>	$g1$	0,26	
<Ставлення керівництва держави до питань забезпечення кібербезпеки>	$a1$	0,75	1,0
<Стан розвитку політики кіберзахисту>	$a2$	0,25	
<**СТАН СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ ДЕРЖАВИ**>	$g2$	0,25	
<Рівень освіти, науки та техніки>	$b1$	0,68	1,0
<Рівень розвитку інноваційного середовища>	$b2$	0,32	
<**НАЯВНІСТЬ РОЗГАЛУЖЕНОЇ ТЕХНОЛОГІЧНОЇ ІНФРАСТРУКТУРИ**>	$g3$	0,26	
<Якісний стан технологічної інфраструктури>	$c1$	0,22	1,0
<Рівень впровадження технологічної інфраструктури>	$c2$	0,78	
<**СТУПІНЬ ВИКОРИСТАННЯ ІКТ ТА ІТС**>	$g4$	0,23	
<Використання інформаційно-комунікаційних технологій>	$d1$	0,71	1,0
<Використання ресурсів мережі Інтернет>	$d2$	0,29	

При цьому значення категорій та індикаторів якості визначаються у спосіб наведений у табл. 3 [2].

За формулами (2), (3), (5), (6), (8), (9), (11) та (12), що приведені у таблиці 3, з використанням даних анкети експерта (табл. 4), що регламентує значення показників та їхніх вагових коефіцієнтів обчислюються значення індикаторів 3-го рівня таких, як:

- <ставлення керівництва держави до питань забезпечення кібербезпеки>;
- <стан розвитку політики кіберзахисту>;
- <рівень освіти, науки та техніки>;
- <рівень розвитку інноваційного середовища>;
- <якісний стан технологічної інфраструктури>;
- <рівень фінансування технологічної інфраструктури>;
- <використання інформаційно-комунікаційних технологій>;
- <використання ресурсів мережі Інтернет>.

Процедури визначення категорій та індикаторів рівня критичності кібербезпеки Таблиця 3

$<\text{НАЯВН. НОРМАТ.–ПРАВОВ. БАЗИ}>=\begin{matrix}a1<\textit{ставлення керівництва до кібербезпеки}>\\ +a2<\textit{стан розвитку політики кіберзахисту}>\end{matrix}$, де $a1$, $a2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $a1+a2=1$;	(1)
$<\textit{Ставлення керівництва до кібербезпеки}>=a1_1\cdot A1_1+a1_2\cdot A1_2+a1_3\cdot A1_3+a1_4\cdot A1_4=\sum_i a1_i\cdot A1_i$; $i=\overline{1,4}$, де $a1_1$, $a1_2$, $a1_3$, $a1_4$ – вагові коефіцієнти показників 4-го рівня для $A1_1$, $A1_2$, $A1_3$ та $A1_4$; $a1_1+a1_2+a1_3+a1_4=\sum_i a1_i=1$;	(2)
$<\textit{Стан розвитку політики кіберзахисту}>=a2_1\cdot A2_1+a2_2\cdot A2_2=\sum_i a2_i\cdot A2_i$; $i=\overline{1,2}$, де $a2_1$, $a2_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $A2_1$ та $A2_2$; $a2_1+a2_2=\sum_i a2_i=1$.	(3)
$<\text{СТАН СОЦІАЛ.–ЕКОНОМ. РОЗВИТКУ}>=\begin{matrix}b1<\textit{рівень освіти, науки, техніки}>\\ +b2<\textit{рівень розвитку інновац. середовища}>\end{matrix}$, де $b1$, $b2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $b1+b2=1$;	(4)
$<\textit{Рівень освіти, науки, техніки}>=b1_1\cdot B1_1+b1_2\cdot B1_2+b1_3\cdot B1_3+b1_4\cdot B1_4=\sum_i b1_i\cdot B1_i$; $i=\overline{1,2}$, де $b1_1$, $b1_2$, $b1_3$, $b1_4$ – вагові коефіцієнти показників 4-го рівня для $B1_1$, $B1_2$, $B1_3$ та $B1_4$; $b1_1+b1_2+b1_3+b1_4=\sum_i b1_i=1$;	(5)
$<\textit{Рівень розвитку інновац. середовища}>=b2_1\cdot B2_1+b2_2\cdot B2_2+b2_3\cdot B2_3=\sum_i b2_i\cdot B2_i$; $i=\overline{1,3}$, де $b2_1$, $b2_2$, $b2_3$ – вагові коефіцієнти показників 4-го рівня для $B2_1$, $B2_2$ та $B2_3$; $b2_1+b2_2+b2_3=\sum_i b2_i=1$.	(6)
$<\text{НАЯВН. РОЗГАЛУЖ.ТЕХНОЛ. ІНФРАСТР.}>=\begin{matrix}c1<\textit{якісний стан технологіч. інфрастр.}>\\ +c2<\textit{рівень впровадж. технологіч. інфрастр.}>\end{matrix}$, де $c1$, $c2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $c1+c2=1$;	(7)
$<\textit{Якісний стан технологіч. інфрастр.}>=c1_1\cdot C1_1+c1_2\cdot C1_2=\sum_i c1_i\cdot C1_i$; $i=\overline{1,2}$, де $c1_1$, $c1_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $C1_1$ та $C1_2$; $c1_1+c1_2=\sum_i c1_i=1$;	(8)
$<\textit{Рівень впровадж. технологіч. інфрастр.}>=c2_1\cdot C2_1+c2_2\cdot C2_2=\sum_i c2_i\cdot C2_i$; $i=\overline{1,2}$, де $c2_1$, $c2_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $C2_1$ та $C2_2$; $c2_1+c2_2=\sum_i c2_i=1$.	(9)
$<\text{СТУПІНЬ ВИКОРИСТ. ІКТ та ІТС}>=\begin{matrix}d1<\textit{використання ІКТ}>\\ +d2<\textit{Використання мережі Інтернет}>\end{matrix}$, де $d1$, $d2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $c1+c2=1$;	(10)
$<\textit{Використання ІКТ}>=d1_1\cdot D1_1+d1_2\cdot D1_2=\sum_i d1_i\cdot D1_i$; $i=\overline{1,2}$, де $d1_1$, $d1_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $D1_1$ та $D1_2$; $d1_1+d1_2=\sum_i d1_i=1$;	(11)
$<\textit{Використання мережі Інтернет}>=d2_1\cdot D2_1+d2_2\cdot D2_2=\sum_i d2_i\cdot D2_i$; $i=\overline{1,2}$, де $d2_1$, $d2_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $D2_1$ та $D2_2$; $d2_1+d2_2=\sum_i d2_i=1$.	(12)

Примітка: вираз < x > позначає числове значення показника властивості x.

Анкета експерта для оцінювання рівня критичності кібербезпеки Таблиця 4

Позначення показника	Питання, на які повинен відповісти експерт для визначення значення показника	Відповіді на питання	Знач. показника	Позначення вагового коефіцієнта показника	Знач. вагового коеф-та показника
1	2	3	4	5	6
$A1_1$	Чи існує в державі національна стратегія (доктрина, концепція тощо) з кібербезпеки?	1) Стратегія зрозуміла з чітко визначеними цілями та термінами реалізації.	1,0	$a1_1$	0,4
		2) Стратегія нечітка, незрозуміла або формальна.	0,4		
		3) Стратегія тільки розробляється.	0,2		
		4) Стратегія відсутня.	0		
$A1_2$	Чи функціонує у державі система нормативно-законодавчого забезпечення сфери кібербезпеки?	1) Законодавство охоплює усі аспекти кібербезпеки.	1,0	$a1_2$	0,3
		2) Є певні закони, проте виконуються лише окремі з них.	0,6		
		3) Є певні закони, проте жоден з них не виконується.	0,2		
		4) Законодавство не сформовано.	0		
$A1_3$	Чи виконуються на державному рівні міжнародні зобов'язання у сфері кібербезпеки?	1) Держава практично виконує міжнародні угоди.	1,0	$a1_3$	0,2
		2) Держава ратифікувала підписані міжнародні угоди.	0,6		
		3) Держава приєдналася до міжнародних угод.	0,2		
		4) Держава не має підписаних міжнародних зобов'язань.	0		
$A1_4$	Чи має місце співробітництво державних і приватних структур у сфері кібербезпеки?	1) Держава прикладає значні зусилля для розвитку державно-приватного співробітництва.	1,0	$a1_4$	0,1
		2) Держава прикладає активні, проте недосконалі зусилля для розвитку державно-приватного співробітництва.	0,5		
		3) Державно-приватне співробітництво не здійснюється.	0		
$A2_1$	Який рівень діяльності керівництва держави у питаннях кіберзахисту?	1) У державі створено орган виконавчої влади, відповідальний за кіберзахист, діяльність якого визнана ефективною.	1,0	$a2_1$	0,5
		2) У діяльності органу виконавчої влади, відповідального за кіберзахист є певні недоліки.	0,5		
		3) Орган виконавчої влади, що має відповідати за кіберзахист у державі відсутній.	0		
$A2_2$	Який рівень діяльності суб'єктів інформаційної і кіберінфраструктури у питаннях кіберзахисту?	1) Рівень реагування суб'єктами інформаційної і кіберінфраструктури на прояви стороннього кібервпливу вищне середнього.	1,0	$a2_2$	0,5
		2) Рівень реагування суб'єктами інформаційної і кіберінфраструктури на прояви стороннього кібервпливу періодичний і спонтанний.	0,5		
		3) Суб'єкти інформаційної і кіберінфраструктури питаннями реагування на прояви стороннього кібервпливу не займаються.	0		
$B1_1$	Яка частка населення у державі має вищу освіту?	1) Висока.	1,0	$b1_1$	0,2
		2) Середня.	0,5		
		3) Низька.	0		
		Визначається як відсоткове відношення молоді віком від 18 до 22 років, яка отримує освіту за денною формою навчання, до загальної кількості студентів зазначеного віку в країні.			
$B1_2$	Яка частка населення у державі володіє іноземною й передусім англійською мовою?	1) Висока.	1,0	$b1_2$	0,2
		2) Середня.	0,5		
		3) Низька.	0		
		Визначається на основі інформації державного центру з вивчення англійської мови.			
$B1_3$	Яка частка НДДКР у державі присвячена дослідженню питань кібербезпеки?	1) Висока.	1,0	$b1_3$	0,3
		2) Середня.	0,5		
		3) Низька.	0		
		Визначається на основі інформації органу держреєстрації НДДКР.			

Продовження табл.4

1	2	3	4	5	6
$B1_4$	Який рівень залучення до виконання НДДКР за напрямом кібербезпеки інженерно-технічного персоналу?	1) Достатній.	1,0	$b1_4$	0,3
		2) Середній.	0,5		
		3) Недостатній.	0		
		Визначається як кількість фахівців, залучених до виконання НДДКР на 1 млн. чоловік населення країни.			
$B2_1$	Який стан витрат у державі на проведення НДДКР в сфері кібербезпеки?	1) Достатній.	1,0	$b2_1$	0,3
		2) Середній.	0,5		
		3) Недостатній.	0		
		Визначається як відношення поточних і капітальних витрат на проведення НДДКР до рівня ВВП.			
$B2_2$	Який стан у державі патентно-раціоналізаторської роботи в сфері кібербезпеки?	1) Достатній.	1,0	$b2_2$	0,4
		2) Середній.	0,5		
		3) Недостатній.	0		
		Визначається як кількість заявок на отримання патентів на 1 млн. чоловік населення країни.			
$B2_3$	Який стан залучення приватного та венчурного капіталу до сфери кібербезпеки?	1) Достатній.	1,0	$b2_3$	0,3
		2) Середній.	0,5		
		3) Недостатній.	0		
		Визначається у відсотковому відношенні приватного та венчурного капіталу до рівня ВВП країни.			
$C1_1$	Який рівень використання мережі Інтернет?	1) Високий.	1,0	$c1_1$	0,5
		2) Середній.	0,5		
		3) Низький.	0		
		Свідчить про кількість Інтернет-користувачів на 100 чоловік та розраховується на основі інформації JiWire (бази даних щодо Wi-Fi – точок доступу у 142 країнах).			
$C1_2$	Який рівень використання засобів мобільного зв'язку та соціальних мереж?	1) Високий.	1,0	$c1_2$	0,5
		2) Середній.	0,5		
		3) Низький.	0		
		Свідчить про кількість користувачів мобільного зв'язку на 100 чоловік та відсоткове відношення кількості користувачів до загальної кількості Інтернет-користувачів.			
$C2_1$	Який рівень фінансування заходів з впровадження ІКТ?	1) Достатній.	1,0	$c2_1$	0,5
		2) Середній.	0,5		
		3) Недостатній.	0		
		Визначається у відсотковому відношенні загальних витрат на програмне забезпечення, апаратні засоби та ІТ-послуги до рівня ВВП.			
$C2_2$	Який рівень безпеки сервісів?	1) Достатній.	1,0	$c2_2$	0,5
		2) Середній.	0,5		
		3) Недостатній.	0		
		Свідчить про кількість серверів , що використовують технології шифрування даних для безпечного обміну даними.			
$D1_1$	Який рівень використання ІКТ у корпоративних мережах?	1) Широке використання корпоративних мереж на всій території країни.	1,0	$d1_1$	0,5
		2) Рівень розвитку корпоративних мереж достатньо високий.	0,6		
		3) Розробляються плани для впровадження корпоративних мереж.	0,2		
		4) Корпоративних мереж у країні не існує.	0		
$D1_2$	Який рівень використання ІКТ у інтелектуальних транспортних системах?	1) Рівень використання ІТС для вирішення важливих функцій високий.	1,0	$d1_2$	0,5
		2) Рівень використання ІТС для вирішення важливих функцій нижче середнього.	0,5		
		3) Інтелектуальних транспортних систем не існує.	0		

Продовження табл. 4

1	2	3		4	5
$D2_1$	Яка частка користувачів використовує Інтернет для розміщення пропозицій щодо надання товарів і послуг?	1) Більше 55 відсотків.	1,0	$d2_1$	0,5
		2) Від 25 до 54 відсотків.	0,5		
		3) Від 0 до 24 відсотків.	0		
$D2_2$	Яка частка користувачів використовує Інтернет для замовлення товарів і послуг?	1) Більше 80 відсотків.	1,0	$d2_2$	0,5
		2) Від 40 до 79 відсотків.	0,5		
		3) Від 0 до 39 відсотків.	0		

Де ВК – ваговий коефіцієнт.

За формулами (1), (4), (7) та (10) табл. 3 з використанням даних табл. 4 та значень отриманих попередньо показників 3-го рівня обчислюються значення комплексних показників (категорій) 2-го рівня, таких як: наявність нормативно-правової бази ($G_1^{факт}$); стан соціально-економічного розвитку держави ($G_2^{факт}$); наявність розгалуженої технолопічної інфраструктури ($G_3^{факт}$); ступінь використання ІКТ та ІТС($G_4^{факт}$).

Комплексний показник оцінювання рівня захищеності держави від стороннього кібернетичного впливу $G_{захищ.}^{рівень}$, або інакше так званий "індекс кіберпотужності" з точки зору одного експерту може бути обчислений за такою формулою [3]:

$$G_{захищ.}^{рівень} = \left(\sum_{i=1}^{n} \left(g_i \cdot G_i^{факт} \right) \right) \cdot 100\%, \qquad (13)$$

де g_i – вагові коефіцієнти категорій другого рівня ієрархії $G_i^{факт}$; n – число категорій (в даному випаду $n = 4$).

Прийняття рішення щодо здатності держави протистояти атакам у кіберпросторі буде здійснюватися на підставі наступного правила:

– якщо $90 \le G_{захищ.}^{рівень} \le 100$, то рівень захищеності держави від ризику стороннього кібервпливу вважається достатньо високим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

– якщо $45 \le G_{захищ.}^{рівень} < 90$, то рівень захищеності держави від ризику стороннього кібервпливу вважається допустимим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

– якщо $G_{захищ.}^{рівень} < 45$, то рівень захищеності держави від ризику стороннього кібервпливу вважається недостатнім.

Висновок. Таким чином, запропонована стратегія дасть можливість одержати кількісну оцінку рівня захищеності держав від ризику стороннього кібернетичного впливу, встановити вимоги до формування ними власних систем кібернетичної безпеки та розробити заходи спрямовані на підвищення їх результативності. Підставою таким діям може слугувати виявлення відхилень від штатного режиму функціонування державних ІР, ІТ систем і мереж, а також відповідних програмних і апаратних засобів, а саме, наприклад, виявлення ознак:

– виведення з ладу окремих компонентів радіоелектронних систем;

– змінювання алгоритмів функціонування ПЗ систем управління в ІТ системах і мережах;

– несанкціонованих змін у файлах (їх розмірів та останньої дати модифікації);

– порушення безпеки інформаційного обміну, протоколів передачі даних вхідного або вихідного трафіка, а також прав доступу користувачів до ІР;

– уповільнення завантаження та роботи ПЕОМ;

– зменшення обсягів вільної оперативної пам'яті;

– виконання неконтрольованих процесів тощо.

Окрім всього цьому може сприяти виявлення чисельних помилок при завантаженні операційних систем, неможливості збереження файлів у необхідних каталогах, а також незрозумілих системних повідомлень, музикальних і візуальних ефектів.

ЛІТЕРАТУРА

[1]. Бешелев С. Д., Гурвич Ф. Г. Экспертные оценки. – М.: Наука, 1973. – 263 с.

[2]. Бурячок В.Л., Луханин М.И., Митрахович М.М. Методика експертного отбора научно-исследовательских и опытно-конструкторских работ при формировании проектов научно-технических программ // Артиллерийское и Стрелковое Вооружение. – 2007. – Спецвыпуск. – С. 23–29.

[3]. Кини Р.Л., Райфа Х. Принятие решений при многих критериях: предпочтение и замещение. – М.: Радио и связь, 1981. – 346 с.

REFERENCES

[1]. Beshelev S.D., Gurvich F.G. Expert estimate, M.: Nauka, 1973, 263 p.
[2]. Buryachok V.L., Lukhanin M.I., Mitrakhovich M.M. Methodology of expert selection of research and experience works at forming projects of the scientific and technical programs // Artillery and rifle armaments, 2007, Special Edition, P. 23–29.
[3]. KEENEY R.L., RAIFFA H Decisions with Multiple Objectives: Preferences and Value Tradeoff,M.: Radio i svyaz′, 1981, 346 p.

СТРАТЕГИЯ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ГОСУДАРСТВА ОТ РИСКА ПОСТОРОННЕГО КИБЕРНЕТИЧЕСКОГО ВЛИЯНИЯ

В промышленно развитых странах задача оценки уровня защищенности их информационной и киберинфраструктуры от риска постороннего кибернетического воздействия относится к ряду приоритетных. Ее решение сейчас невозможно без комплексного исследования способности систем кибернетической безопасности этих стран противодействовать такому воздействию и его деструктивным последствиям. Прежде всего это объясняется непрерывным ростом объема информации, которая циркулируют, накапливается и обрабатывается в информационных и киберпространствах этих стран, увеличением скоростей ее передачи, бурным развитием новых информационно-телекоммуникационных технологий и общей компьютеризацией, в частности доступом в Интернет, а также необходимостью защиты такой информации от воздействия внутренних и внешних кибернетических вмешательств и угроз. С учетом этого изложено стратегию действий, которая позволит: во-первых - оценить уровень защищенности инфосферы государства от риска постороннего кибервлияния, во-вторых - получить количественное значение "индекса киберпотужности", что характеризует готовность государственных объектов информационной и киберинфраструктуры к безопасному функционированию при таких условиях, в-третьих - установить требования к формированию государственной системы кибернетической безопасности и разработать мероприятия направленные на повышение ее результативности. Установлено, что на степень критичности кибербезопасности к атакам в киберпространстве главным образом влияет наличие сложившейся и четко функционирующей нормативно-правовой базы и разветвленной технологической инфраструктуры страны, состояние ее социально-экономического развития, а также степень использования страной информационно-коммуникационных технологий и систем. Для оценки уровня защищенности предложено использовать метод анкетирования - один из известных методов экспертного оценивания.

Ключевые слова: стратегия оценки, оценка уровня защищенности, кибернетическое влияние, информационно-коммуникационная технология, кибербезопасность, киберугрозы, киберпространство.

AN EVALUATION STRATEGY OF STATE SECURITY LEVEL FROM THE RISK OF EXTERNAL CYBER INFLUENCE

In industrialized countries, the task of protection level evaluation of its information and cyber infrastructure from the external cyber influence refers to the number of priority. The problem solving now is impossible without an integrated study of the systems cyber-security ability of these countries to counter such influence and its destructive effects. First of all it is caused by the continuous increase of the information, that circulates, accumulates and processed in the cyberspaces of these countries, and also by the increase of speed of its transmission, by the rapid development of new information and telecommunication technologies and general computerization, in particular, an access to the Internet, as well as the need to protect information from internal and external cyber threats and interferences. Taking the above mentioned into consideration, it was represented the strategy of actions which will give an opportunity: the first is to evaluate a level of state security from the risk of external cyber influence; the second is to obtain the quantitative value of " Cyber Power Index ", what characterizes the readiness of State objects cyberinfrastructure for safe operation under such conditions; thirdly, to establish requirements for the State systems development of cyber-security and to develop measures aimed to increase its effectiveness. It was established, that the level of cyber security awareness to attacks in cyberspace, mainly depends on the presence of implemented regulatory framework and the substantial technological infrastructure of the country, the condition of its socio-economic development, as well as the usage of information and communication technologies and systems by the country. For protection level evaluation it was offered to use the questionnaire method - one of the known methods of expert assessment.

Keywords: strategy of assessment, protection level evaluation, cyber influence, information and telecommunication technologies, cybersecurity, cyber threat, cyber space.

Бурячок Володимир Леонідович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного управління в/ч А 1906.
E-mail: BVL-home@ua.fm
Бурячок Владимир Леонидович, кандидат технических наук, старший научный сотрудник, начальник научно-исследовательского управления в/ч А 1906.
Buryachok Volodymyr, Senior Researcher, PhD in Eng., Head of Research department M/P A 1906.

Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Корченко Александр Григорьевич, доктор технических наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
Korchenko Alexander, Professor, Doctor of Science in Eng., Head of Academic Department of IT-Security, National Aviation University.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: Professor_va@ukr.net
Хорошко Владимир Алексеевич, доктор технических наук, профессор, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Horoshko Volodymyr, Professor, Doctor of Science in Eng., Professor of Academic Department of IT-Security, National Aviation University.

Кудінов Вадим Анатолійович, кандидат фізико-математичних наук, доцент, начальник кафедри інформаційних технологій Національної академії внутрішніх справ України.
E-mail: icaocentre@nau.edu.ua
Кудинов Вадим Анатольевич, кандидат физико-математических наук, доцент, начальник кафедры информационных технологий Национальной академии внутренних дел Украины.
Kudinov Vadym, PhD in physics, associate professor, head of Department of Information technology of the National Academy of Internal Affairs Ukraine.

УДК 004.891:65.012.8(045)

МЕТОДОЛОГІЯ СИНТЕЗУ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Олександр Корченко, Максим Луцький, Марія Захарова, Юрій Дрейс

Анотація. *Віднесення відомостей до державної таємниці проводиться державним експертом з питань таємниць шляхом встановлення, обґрунтування та визначення величини можливої шкоди національній безпеці держави у разі їх розголошення для прийняття рішення щодо ступеня їх секретності. Існуючі засоби розрахунку такої шкоди в переважній більшості базуються на отримання умовної (бальної) оцінки її прогнозованої величини. У роботі представлено методологію синтезу системи аналізу і оцінки величини можливої шкоди національній безпеці держави, яка дозволяє на основі моделі інтегрованого представлення параметрів шкоди, отриманих існуючими засоби аналізу у сфері охорони державної таємниці, оцінювати шкоду як в умовних (бальних) одиницях, так і в вартісній (грошовій) величині збитку. Основана вона на розроблених методах: аналізу і оцінки шкоди національній безпеці у сфері охорони державної таємниці, оцінювання важливості відомостей за визначеними сферами державної таємниці, визначення рівня компетентності членів експертної комісії при державних експертах з питань таємниць. Окрім цього, методологія дає можливість відображати результати як в якісній, так і в кількісній формі, наприклад, з використанням лінгвістичних змінних, що часто вживаються для опису складних систем. Програмна реалізація системи з інтегрованою базою даних існуючих засобів дає змогу провести аналіз і оцінку величини можливої шкоди національній безпеці держави з додатковими можливостями автоматизованого формування звіту її результатів.*

Ключові слова: *державна таємниця; оцінка шкоди; методологія системи аналізу і оцінки величини можливої шкоди національній безпеці держави; охорона державної таємниці; параметри шкоди.*

Відомо, що методологічний базис є найважливішим компонентом теорії захисту інформації (ЗІ) [1], який складається з сукупності методів і моделей, необхідних і достатніх для досліджень проблеми ЗІ і вирішення практичних завдань відповідного призначення. В зв'язку з цим на особливу увагу заслуговують завдання аналізу і оцінки величини можливої шкоди (АОШ) національній безпеці держави у сфері охорони державної таємниці (ОДТ) [2]. Проте, при практичному використанні існуючих засобів АОШ [3-5] члени експертної комісії при державних експертах з питань таємниць (далі – ДЕТ) не завжди можуть чітко детермінувати оціночні параметри, оскільки їх часто виражають в якісній формі. Тому особливий інтерес представляють системи [6], які до-