ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.26.14974

КІЛЬКІСНО-ЯКІСНА ОЦІНКА ТА ВИЗНАЧЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ДЕРЖАВИ

Пискун І.В.[1], Ткач Ю.М.[2], Хорошко В.О.[3], Хохлачова Ю.Є.[3], Аясрах А.[3], Аль-Далваш А.[3]

[1]Державний університет інформаційно-комунікаційних технологій
[2]Чернігівський національний технологічний університет
[3]Національний авіаційний університет

ПИСКУН Ігорь Васильович

Рік та місце народження: 1973 рік, м. Київ, Україна.
Освіта: Державний університет інформаційно-комунікаційних технологій, 2009 рік.
Посада: науковий співробітник Національного авіаційного університету.
Наукові інтереси: інформаційна безпека та управління інформаційною безпекою.
Публікації: більше 20 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: 0223910@gmail.com.
Orcid ID: 0000-0001-8616-3414.

ТКАЧ Юлія Миколаївна, д.пед.н., професор

Рік та місце народження: 1979 рік, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет, 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001рік.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 рік.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
Orcid ID: 0000-0002-8565-0525.

ХОРОШКО Володимир Олексійович, д.т.н., професор.

Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функіонування складних систем.
Публикации: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

ХОХЛАЧОВА Юлія Євгеніївна, к.т.н., доцент.

Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, оцінювання уразливостей, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: hohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

АЯСРАХ Ахмад Расмі Алі

Рік та місце народження: 1992 рік, м. Джераш, Йорданія.
Освіта: Київський національний університет будівництва і архітектури, 2019 рік.
Посада: аспірант, Національний авіаційний університет.
Наукові інтереси: інформаційна безпека, кібербезпека в інформаційних системах.
Публікації: 3 наукових публікації, серед яких наукові статті та тези.
E-mail: ahmadaesr@gmail.com.
Orcid ID: 0000-0003-4392-1806.

АЛЬ-ДАЛВАШ Аблуллах Фоуад

Рік та місце народження: 1991 рік, м. Самарра, Ірак.
Освіта: Донецький національний університет імені Василя Стуса, 2018 рік.
Посада: аспірант, Національний авіаційний університет.
Наукові інтереси: інформаційна безпека, кібербезпека в інформаційних мережах.
Публікації: 2 наукових публікації, серед яких наукова стаття та тези.
E-mail: abduiiah.dalosh@gmail.com.
Orcid ID: 0000-0001-1003-9182.

Анотація. *В статті розроблено методику кількісно-якісного аналізу та визначення рівня кібербезпеки інформаційних систем держави. Забезпечення кібернетичної безпеки – процес безперервний, надзвичайно складний і багатогранний, причому успіх у його реалізації зумовлюється станом відносин у суспільстві і залежить від кожного його представника, але передусім від здійснення державної політики у цій сфері. Отримані результати достатньо чітко визначають критерій кібернебезпеки, який виходить із чисельних значень індексу кібернебезпеки або кіберзагрози. Критерій оцінки рівня кіберзагрози має опиратися на характер кіберзагрози з обов'язковим урахуванням її масштабу. Обидва показники мають кількісний вимір, однак безпосереднє зведення їх до одного узагальненого показника не має підстав через принципову різницю між явищами, що ними характеризуються. Тому найбільш раціональним шляхом є логічний аналіз. Таким чином, у статті показано, що кожному рівню кіберзагрози відповідає свій рівень кібербезпеки. Отже, критерієм оцінки рівня кібербезпеки є рівень кіберзагрози.*

Ключові слова: *інформаційна безпека, кіберзагрози, кібербезпека, критична інфраструктура, загрози безпеці, когнітивне моделювання, нечітка когнітивна карта.*

Вступ

Інформаційне протиборство не є надбанням сьогоднішнього дня. Історія людства – це історія воєн як найпотужніших засобів перерозподілу цінностей, територій та здобуття контролю над ними. Багато прийомів інформаційного протиборства виникли тисячі років тому разом з появою інформаційних систем – історія навчання людства і є свого роду інформаційним протиборством. При цьому цілком природньо, що з підвищенням можливостей інформаційних систем у частині їх заснування, акцент все більше і більше зміщується у бік застосування систем з кіберзахистом. Існування і розвиток будь-якої держави відбувається в тісному зв'язку з політичними та геополітичними умовами та значною мірою залежить від рівня кібербезпеки в державі.

З появою інформаційно-комунікаційних технологій інформаційно-телекомунікаційних систем світова спільнота отримала не тільки численні переваги, а й цілу низку проблем, з умовлених дедалі більшою вразливістю інформаційного простору що до стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю, та врегулювання відповідних взаємовідносин, а отже, і не відкладного створення надійної системи кібербезпеки. Відсутність такої системи може призвести до втрати політичної незалежності будь якої держави світу, бо йтиметься про фактичний програш нею змагання не військовими засобами та підпорядкування її національних інте-

ресів стороною, яка здійснює ці дії. Оскільки самі ці обставини відіграють, останнім часом важливу роль у геополітичному протиборстві та конкуренції більшості держав світу, то забезпечення кібербезпеки стає головним завдання сьогодення.

Вирішення проблем забезпечення кібербезпеки держави неможливо без постійного аналізу відносин у суспільстві, районі, регіоні, державі та світі, виявлення (прогнозування) на цій основі кібербезпеки, що існує або може виникнути, та вжиття адекватних заходів щодо її реалізації.

Відомо, що відносини у суспільстві – це конкретний стан відносин у регіоні, між партіями, соціальними групами, пов'язані зі створенням та використанням можливостей відтворення кіберзагроз і кібератак [1]. При цьому обов'язково слід враховувати терористичні та кібернетичні атаки на різні інформаційні ресурси.

Оцінка відносин у суспільстві має характер науково-теоретичного пізнання та опирається на такі методологічні принципи [2]:

- об'єктивність та реалістичність наведеної інформації;

- всебічність та комплексний аналіз отриманої інформації;

- конкретний підхід відносно отриманої та опрацьованої інформації.

Однак реалізація цих принципів потребує обґрунтованих методичних підходів і прийомів для визначення дійсних справ, фактичного співвідношення сил, тенденцій розвитку подій, за якими стоять певні інтереси, можливості та дії.

Аналіз публікацій та досягнень. Зараз активізувалась робота з оцінки рівня кібербезпеки із застосуванням математичних методів [1,2,3,4,5]. Проте існуючі моделі і методи далекі від досконалості.

До цього часу не існує адекватної методики оцінки як кількісного, так і якісного рівня кібернетичної безпеки.

Основними проблемами, які необхідно розв'язати для методик кількісно-якісного аналізу ситуаційної обстановки та визначення рівня кібербезпеки, є:

- визначення функціональної залежності між кількісними значеннями часткових показників обстановки навколо інформаційної системи та індексом кібербезпеки;

- розробка критерію оцінки рівня кібербезпеки, виходячи з усієї сукупності її якісних та кількісних характеристик;

- визначення методики обґрунтування пріоритетних заходів, спрямованих на забезпечення необхідного рівня кібербезпеки.

В роботах [3,4,5] розглядаються методики кількісно-якісного аналізу та визначення рівня інформаційної безпеки. При цьому враховуються апаратно-програмні, апаратні та програмні методи та засоби захисту інформації. Крім цього слід ще враховувати адміністративні та організаційно-технічні засоби. А при оцінці кібербезпеки, яка є складовою частиною інформаційної безпеки, враховувати тільки програмні та криптографічні методи та засоби. Також, при проведенні кількісно-якісного аналізу кібернетичної безпеки необхідно враховувати імовірність використання зловмисником окрім несанкціонованого доступу до інформації також хакерські та вірусні атаки. Це дуже важливо тому, що при несанкціонованому доступі зловмисник може отримати інформацію та її змодефікувати, а при хакерській або вірусній атаці інформація може бути пошкоджена, модифікована або знищена. Причому, хакерські та вірусні атаки можуть бути такі, як DoS, DDoS, Logic bombs, Phishing, Wanna Cry, Win32/Stuxnet, Worm, Flame, Virus Petya та інші. З урахувань цих положень і вирішується кількісно-якісна оцінка рівня кібербезпеки інформаційних систем держави.

Мета роботи

Мета роботи – розробка методики кількісно-якісного аналізу та визначення рівня кібербезпеки інформаційних систем держави.

Основна частина. Формальне представлення задачі дослідження можна зазначити як пошук та визначення залежності

$$y = f(x_1, x_2, \dots, x_k), \qquad (1)$$

де y – цільова функція об'єкта дослідження;
$(x_1, x_2, \dots, x_k)$ – чинники, які суттєво впливають на стан об'єкта дослідження;
k – загальна кількість чинників, що розглядається.

Залежність (1) пов'язує цільову функцію з основними чинниками, які впливають на її значення, тобто є математичною моделлю об'єкта дослідження. Кожен з фіксованих наборів чинників визначає конкретне значення цільової функції .Таким чином, пошук раціональних шляхів забезпечення кібербезпеки полягає у визначенні такої сукупності $x_1, x_2, \dots, x_k$, яка забезпечує наближення до максимального значення цільової функції y за умови існуючих обмежень.

Слід відзначити, що такою цільовою функцією може бути індекс кібербезпеки. Способи визначення величин, що визначені у [3] для обчислення індексу кібербезпеки, можуть бути різними. Найпростішим шляхом є проведення експертних оцінювань, але більш ґрунтовні та достовірні оцінки можуть бути отримані за допомогою функціональної залежності індексу кібербезпеки від об'єктивних кількісних характеристик суспільної обстановки та інших факторів, що впливають на кібербезпеку.

Першим кроком до розвитку індексу кібербезпеки має бути визначення індексу кіберзагрози, як ймовірності заподіяння суттєвої шкоди, яка є власністю людини, підприємства, організації або держави. Така ймовірність має у своїй основі імовірність самої атаки. У свою чергу, кібератаку та інформацію можна ототожнити з прийняттям зловмисником-ініціатором кібератаки рішенням про атаку.

Важливу роль у визначенні індексу кібербезпеки відіграє врахування можливостей носіїв інформації та самої інформації – об'єкта потенційної кібератаки щодо її отримування та відбиття. При цьому слід враховувати особливості кібератак [1], які можуть бути як хакерські так і вірусні.

Таким чином, опираючись на міркування, наведені у [3,4], розрахунок індексу кібербезпеки у взаємовідносинах двох суб'єктів (назвемо їх сторонами A і

B) можна звести до визначення імовірності прийняття потенційного порушника або зловмисника (нехай ним буде сторона *A*) рішення про здійснення кібератаки того чи іншого масштабу проти сторони В та імовірності успіху кібератаки за умов конкретних можливостей сторони В щодо її відбиття або відвернення кібератаки.

З урахуванням досліджень, проведених у [4], та підходу до кількісно-якісної оцінки навколишньої ситуації не явного об'єкту, головними висновками з такої оцінки можуть бути:

- співвідношення "виграш-програш" для сторони *A*, тобто величина K_{ex}^{AB} ;

- співвідношення сил сторін, тобто величина G^{AB}.

На підставі цих висновків, а також інших об'єктивних та суб'єктивних факторів рішення сторони *A* про початок кібератаки на інформацію сторони *B* може бути прийняте або не прийняте. Певний вплив на це рішення буде чинити, зокрема рівень підготовки до готовністю сторони *A* до позитивного сприйняття такого кроку стосовно сторони В.

Таким чином, рішення про кібератаку слід вважати подією, імовірність настання якої на прогнозований час визначається, головним чином, переліченими раніше факторами та умовами. Цю імовірність можна ототожнити з імовірністю кібератаки, яку в [3,4] позначено через $P_{АТАК}$. Оскільки здійснення кібератаки та її відвернення можливо описати як:

$$P_{АТАК} = 1 - P_{відб} = 1 - [(1 - P_{пас})(1 - P_{акт}], \quad (2)$$

де $P_{АТАК}$ – імовірність протидії кібератаки на інформацію, при цьому слід враховувати ще і несанкціонований доступ хакерські та вірусні атаки;

$P_{відб}$ – імовірність відбиття кібератаки на інформацію;

$P_{пас}$ – імовірність пасивного відбиття кібератаки на інформацію;

$P_{акт}$ – імовірність активного відбиття кібератаки на інформацію.

Але крім протидії кібератакам (відбиттям) треба ще враховувати і ймовірність порушення системи кіберзахисту зловмисниками, яку можна визначити [2] як:

$$P_{ПСЗ} = 1 - (1 - P_{пк})(1 - P_{пц})(1 - P_{пд}), \quad (3)$$

де $P_{пк}$ – імовірність порушення конфіденційності;

$P_{пц}$ – імовірність порушення цілісності;

$P_{пд}$ – імовірність порушення доступності.

Тобто, вираз (2) приймає вигляд:

$$P_{АТАК} = 1 - [(1 - P_{пас})(1 - P_{акт})(1 - P_{псз})]. \quad (4)$$

Слід зазначити, що питання, пов'язані з $P_{пк}$, $P_{пц}$, $P_{пд}$, вже дуже докладно та глибоко розглянуті в [2]. Тому зараз, у зв'язку з обмеженим обсягом статті, ми їх тільки використовуємо, без детального розгляду.

Розглянемо рівняння (4) з точки зору залежності співмножників, що входять до його правої частини, від перелічених раніше показників обстановки, приводить до таких висновків:

По-перше, відбиття кібератаки зводиться по суті, до зменшення величини, тобто до наближення, наскільки це можливо до балансу інтересів сторін *A* і *B*. Досягнення цієї мети сприятиме шляхами та засобами прогнозованої величини L^{AB}. Загальним результатом буде зменшення коефіцієнта проникнення $K_{про}^{AB}$, який враховує показники виразу (3).

Крім того, слід врахувати, що $K_{про}^{AB} = \frac{V^{AB}}{L^{AB}}$,

де V^{AB} – виграш сторони *A*;

L^{AB} – збиток, який зазнає сторона *A* в ході кібератаки на інформацію сторони *B*.

По друге, активне відбиття можливої кібератаки, так само як і її відбиття, досягається головним чином, шляхом забезпечення відповідного співвідношення сил з урахуванням очікування кібератаки.

Таким чином, між значенням $K_{про}$ і *G* (під час подальших досліджень індексом *A* і *B* для спрощення запису будуть випущені) та імовірністю $P_{АТАК}$ існує пряма залежність. Очевидно, що зростання величини $K_{про}$ і *G* веде до зростання величини $P_{АТАК}$ і навпаки. Проте ні характер цієї залежності, ні тим більше функціональний зв'язок між зазначеними показниками і величиною $P_{АТАК}$ невідомі.

Для вирішення шляхів вирішення поставлених питань доцільно звернутися до теорії прийняття рішень [6].

Відповідно до [6] у разі задач з ризиком особа, яка приймає рішення (ОПР), створює власне евристичне уявлення щодо задачі як список факторів (вимірів), що включає величину виграшу, величину програшу, імовірність програшу та рівень ризику. Рішення, за твердженням [4,6], є функцією двох основних змінних величини: величин виграшу (ВВ) та ризику (R). У результаті проведених досліджень встановлено, що під час оцінювання ризику беруть до уваги, головним чином, величину програшу (ВП) та суб'єктивну імовірність програшу (СІП). Для умов, визначених в [3,4,5] досліджень емпірична залежність для оцінки величини ризику визначається рівнями (для інформаційної безпеки):

$R = 3{,}12(\text{СІП}) + \lg(\text{ВП})$, а для кібербезпеки величина ризику буде:

$$R = 3{,}26(\text{СІП}) + \lg(\text{ВП}). \quad (5)$$

За твердженням [3,4,5], формула (5) має велику прагматичну цінність. Коефіцієнт кореляції між оцінками, отриманими за допомогою (5), та оцінка авторів склала біля 0.95, що свідчить про високу точність прогнозу. Відповідь на запитання про те, як сполучення величин виграшу ВВ та ризику R впливає на відсоток, який приймає запропоновані умови виграшу та ступінь ризику, дає рівняння регресії за [7]:

$$D(\%) = 1{,}47(BB) - 49{,}25(R) + 146, \quad (6)$$

де отримано за підсумками проведених досліджень. При цьому, з урахуванням особливостей кібератак та кіберзахисту [1,2], коефіцієнт кореляції між оцінками, одержаних за допомогою (6) та даними досліджень, склав 0.9, що також є доказом високої збіжності.

Віддаючи належне коректності результатів, одержаних [3,5], слід у той самий час зауважити, що в інтересах даного дослідження ці результати не можуть бути використані без застережень. Справа в тому, що умови проведення описаних в [3,5] експериментів, які полягали в пред'явленні їх учасником альтернатив у вигляді виграшу у сполученні з певним ризиком програшу, не можна співставляти з умовами прийняття найважливіших рішень зловмисником. Крім того, в сфері інформаційних відносин виграш або програш (збиток) далеко не завжди може мати пряме матеріальне обчислення. Однак у теорії прийняття рішень

вимагається практично загальновизнаним той факт, що фундаментальні закони, які визначають процес оцінки альтернатив, не зазнають модифікації, під впливом змінювання цілей оцінки прийняття рішень (ОПР). Модифікація структури цілей може спричинити кількість, але не якісні зміни [7]. Тому загальний характер експериментально встановлених залежностей між значенням можливого виграшу та ступеня ризику, з одного боку, та імовірністю прийняття ОПР таких умов, з іншого боку, можна екстраполювати і на умови задачі, яка розглядається.

Використання виявлених в [3,4,5,8] закономірностей для вирішення поставлених у даному дослідженні завдань може бути аргументовано ще й таким чином: на рівні буденної свідомості щодо кібербезпеки висновки [7] можна вважати адекватним.

Розглянуті результати досліджень у галузі теорії прийняття рішень [6], у сукупності із запропонованим у [3,4,8] підходом до визначення чисельних значень показників кіберзагрози і кібербезпеки, можуть бути основою для визначення функціональної залежності між імовірності початкузабезпечення кібербезпеки і такими показниками відношеннями в суспільстві як коефіцієнт проникнення $K_{\text{про}}$ та співвідношення сил, тобто залежності:

$$P_{\text{АТАК}} = f\left(K_{\text{про}}, G\right). \quad (7)$$

Слід припустити, що за фіксованих значень $K_{\text{про}}$ існує певна залежність $P_{\text{АТАК}}$ від абсолютних значень V і L, яка виявляється у зростанні $P_{\text{АТАК}}$ при переміщенні величин V і L в область мінімальних або максимальних значень.

Крім цього, пропорційне одночасне зміщення величин V і L в область менших або більших значень без зміни величин $K_{\text{про}}$ означає відповідні зміни в менший або більший бік зловмисних цілей потенційного нападника, так і прогнозованих втрат сторін у випадку зловмисних дій. Останні, в свою чергу, значною мірою залежать від рівнів технічного забезпечення сторін. З огляду на це певне зростання в обох випадках величини $P_{\text{АТАК}}$ можна пов'язати з дією відмічених у [5,8] закономірностей щодо впливу рівнів технічної оснащеності сторін на імовірність виникнення зловмисних дій [9].

Проведений аналіз дає змогу стверджувати, що задача об'єктивної кількісної оцінки імовірності протидії кібератаки на інформацію однією зі сторін одержала задовільне рішення, яке подано залежністю:

$$P_{\text{АТАК}} = \frac{1}{1+\frac{3e}{K_{\text{про}}G}e^{1-K_{\text{про}}}}. \quad (8)$$

Наступним кроком на шляху до визначення індексу кібербезпеки є кількісна оцінка імовірності успіху несанкціонованих і зловмисних дій у випадку кібератаки на інформацію.

Успіх (не відбиття) кібератаки є подією, протилежною її успішного відбиття. Якщо позначити імовірність не відбиття кібератаки $P_{\text{нвід}}$, то очевидно, що

$$P_{\text{нвід}} = 1 - P_{\text{від}}. \quad (9)$$

При цьому ще слід враховувати рівняння (3).

Таким чином, питання зводиться по суті, до визначення величини $P_{\text{від}}$.

Рівняння [4]:

$$P_{\text{від}} = P_{\text{лок}} + P_{\text{від(лок)}} + P_{\text{рег}} + P_{\text{від(рег)}} + \\ + P_{\text{нац}} + P_{\text{від(нац)}} + P_{\text{глоб}} + P_{\text{від(глоб)}}, \quad (10)$$

де $P_{\text{від(лок)}}$, $P_{\text{від(рег)}}, P_{\text{від(нац)}}, P_{\text{від(глоб)}}$ – імовірності відбиття атаки на інформацію відповідного характеру. Це рівняння для розрахунку $P_{\text{від}}$ містить кілька додатків, значення яких залежить від імовірностей небуття можливої кібератаки того або іншого масштабу та імовірності її відбиття за відповідних умов.

Порядок визначення масштабу кібератаки на інформацію розглянуто у [3,4,8]. Однак значення цього показника слід розглядати як математичне очікування випадкової величини, що розглядається згідно з відповідним законом. Такий висновок ґрунтується на залежності масштабу кібератак на інформацію від великої кількості випадкових факторів. Саме з тих причин рівняння (8) враховує різні умови відбиття кібератак.

Щодо закону розподілу масштабу кібератаки, що за умови відсутності статичних даних доцільно віддати перевагу нормальному закону розподілу як найбільш загальному, оскільки немає підстав для того, щоб робити інші припущення. З урахуванням цього математична залежність для розрахунку цільності розподілу імовірності масштабу атаки матиме такий вигляд:

$$f(M_{\text{атак}}) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(M_{\text{атак}}-M_{\text{очік}})^2}{2\delta^2}}, \quad (11)$$

де $M_{\text{атак}}$ – масштаб кібератак на інформацію (випадкова величина); $M_{\text{очік}}$ – математичне очікування кібератаки на інформацію (порядок його визначення розглянуто у роботах [3,4]).

Дослідження залежності ходу та результату відбиття кібератаки від співвідношення сил є важливою методологічною проблемою. Залежно від масштабу та конкретних умов кібератаки для розв'язування цієї задачі застосовуються різні методичні підходи. Проте загальний характер залежності успіху від співвідношення сил зберігається за будь-яких умов, і, на думку фахівців, зводиться до так званої "логічної функції", графік якої становить собою S-подібну криву. Тому в інтересах наближеної оцінки впливу співвідношення сил на успіх відбиття кібератаки доцільно звернутися до залежності [8]:

$$U = \frac{F}{1+al^{-bt}}, \quad (12)$$

де U – значення шуканої величини залежно від значення змінної величини t;

F – верхня межа росту величини U;

t – зміна величина (аргумента);

l – основа натуральних логарифмів;

a – безрозмірна константа;

b – константа, що має розмірність $\frac{1}{t}$.

З урахуванням прийнятих позначень ($K_{\text{про}}$ є аналогом змінної величини t), рівняння (10) набуває такого вигляду:

$$P_{\text{АТАК}} = \frac{1}{1+ae^{-bK_{\text{про}}}}. \quad (13)$$

Тобто слід прийняти b=G, тому чим більше G, тим менше ступінь ризику і є механізмом взаємо ком-

пенсації величини ризику і величини виграшу, що має важливе значення у теорії прийняття рішень [6].

А для виявлення смислового значення величини "a" звернемо увагу на таке. Очевидно, що при $K_{\text{про}} = 0$ і/або $G = 0$, $P_{\text{АТАК}} = \frac{1}{1+a}$.

Але оскільки також очевидно, що величина $P_{\text{АТАК}}$ дорівнює за цих умов нулю, слід визначити, що величина "a" повинна мати нескінченно велике значення. Тому може бути цілком логічним висновок про те, що за умови даної задачі величина "a" повинна мати нескінченно велике значення.

Тому може бути цілком логічним висновок про те, що за умови даної задачі величина "a" не є константою. Вона залежить від $K_{\text{про}}$ та G і при $K_{\text{про}} \to 0$ та/або $G \to 0$ набуває такого значення, яке наближається до нескінченної величини. Отже, величина "a" має бути обернено пропорційною величинам $K_{\text{про}}$ і G.

Баланс інтересів, який характеризується близькими до нуля значеннями $K_{\text{про}}$ і визначає стабільність на основі балансу інтересів, має головною особливістю відсутність вираженої кіберзагрози незалежно вираженої кіберзагрози незалежно від наявності або відсутності балансу сил.

Стабільність на основі балансу сил, коли $0< K_{\text{про}}<1$ є менш стійким станом, який характеризується наявністю потенційної кібербезпеки. При цьому величина $P_{\text{АТАК}}$ може досягати значення 0.35.

Не можна звернути увагу і на таке питання, як рівень ефективності системи кібербезахисту та технічних можливостей зловмисника, відповідно до якого досягнуто балансу сил.

Таким чином, навіть за наявності балансу сил, зростання рівня технічних можливостей сторін об'єктивно підвищує імовірності можливості кібератаки на інформацію.

Так виявляється стримуючий вплив технічних можливостей сторін з точки зору відвернення кібератак. І навпаки, зниження рівня технічних можливостей сторін може привести до такого зростання величини $K_{\text{про}}$, за яким кібератака може відбутися навіть з незначного приводу з відповідним об'єктивним зменшенням масштабу втрати інформації.

Відносна стабільність на основі стимулювання ($K_{\text{про}} > 1, G = 1$) означає зростання інформаційної кібербезпеки (кіберзагрози) до реальної.

При $K_{\text{про}}$ = 1.5, $G = 1$ імовірність здійснення кібератаки може досягати значення 0,45. За цих умов порушення балансу сил, тобто перехід величини G в область значень, які суттєво перевершують одиницю, веде до різкого зростання $P_{\text{АТАК}}$, що згідно з прийнятою класифікацією, означає нестабільність на основі дисбалансу сил та інтересів.

При цьому таку $P_{\text{АТАК}}$ можна пов'язувати з кібератакою або безпосередньо загрозою інформації.

Залежність (10) була використана від час формалізації задачі визначення імовірності відбиття кібератаки. Стосовно оцінки імовірності відбиття атаки ця залежність набуває такого загального визначення:

$$P_{\text{від}} = \frac{1}{u+ae^{-bG_{\text{об}}}}. \quad (14)$$

Сформулюємо вихідні положення для уточнення (14):

1. При $G_{\text{об}} \to 0$ величина $P_{\text{від}}$ має наближатися до нульового значення.

2. При $G_{\text{об}} \to \infty$ величина $P_{\text{від}}$ має наближатися до одиниці.

3. При $G_{\text{об}} \to 1$ (тобто коли умови не віддають перевагу жодній із сторін) повинно виконуватися рівняння $P_{\text{від}} = 0{,}5$.

Задача зводиться до визначення величини "a" і "b" таким чином, щоб це відповідало поставленим вимогам.

Очевидно, що величина "a" повинна бути обернено пропорційно співвідношенню сил; крім того, при $G_{\text{об}} \to 1$ має бути справедливим рівняння

$$ae^{-b} = 1. \quad (15)$$

Значення константи "b" слід установити рівним одиниці, оскільки, крім співвідношення сил, залежність (14) не передбачає урахування будь-яких інших факторів обстановки. Тоді з (15) витікає, що у загальному випадку $a = \frac{e}{G_{\text{об}}}$ залежність (14) у кінцевому вигляді може бути записана як:

$$P_{\text{від}}^{M} = \frac{1}{1+\frac{1}{G_{\text{об}}^{M}}e^{1-G_{\text{об}}^{M}}}. \quad (16)$$

Необхідно мати на увазі, що принципова умова коректності виконання виразів (14) і (16) полягає в тому, що при рівних шансах протиборчих сторін на успіх мало місце рівняння $G_{\text{об}} = 1$. Однак, як вже відзначалося у [3,4,8], це не завжди так, особливо в умовах дуже корисної та разової кібератаки на конкретний інформаційний об'єкт. Таким чином у деяких випадках може виникнути необхідність звернення фактичного значення величини G до такого значення, яке відповідало б фізичному смислу рівності сил у формулі (14). Для цього може бути використана формула зведення:

$$G_{\text{зв}} = GK_{\text{зв}}, \quad (17)$$

де $G_{\text{зв}}$ – зведене значення співвідношення сил;
G – фактичне зведене значення співвідношення сил;
$K_{\text{зв}}$ – коефіцієнт зведення.

У свою чергу коефіцієнт зведення може бути розрахований за формулою:

$$K_{\text{зв}} = \frac{1}{G_{min}}. \quad (18)$$

де G_{min} – мінімально необхідне співвідношення сил для досягнення успіху зловмисником.

Одержані в результаті проведеного аналізу розрахункові співвідношення індексу кібербезпеки за допомогою рівняння (3).

Проте індекс кібербезпеки не має достатньої цінності без зіставлення його з іншими показниками , що характеризують кібербезпеку. Ця проблема може бути сформульована як необхідність вибору критерію оцінки рівня кібербезпеки за всією сукупністю її основних кількісних та якісних характеристик.

У першу чергу, необхідно пов'язати можливі чисельні значення індексу кіберзагрози з прийнятими рівнями стану відносин у суспільстві стабільності в інформаційному просторі та визначеннями характеру кіберзагрози.

Аналіз порівняльних даних щодо ймовірностей відвернення і протидії кібератаці, а також відповідних значень індексів кіберзагроз, розрахованих за допомогою формул (14) та (16), у зіставленні з прийнятими

рівнями стабільності та відносин у суспільстві приводить до висновків наведених в табл. 1:

- потенційній кіберзагрозі відповідають значення індексу кіберзагрозі в мережах $0 \div 0{,}25$;
- стан кіберзагрози інформації або кібератака настає при досягненні індексом значення, яке дорівнює або більше від 0,75, при цьому безпосередній кіберзагрози відповідають значення $P_{\text{кнб}} \geq 0{,}85$.

Проміжні значення $0{,}85 < P_{\text{кнб}} < 0{,}7$ слід віднести до реальної кібернетичної небезпеки.

Таблиця 1

Залежність характеру кіберзагрози
від показників стану відносин у суспільстві

Рівень стабільності у суспільстві	Характерні значення кількісних показників відносин у суспільстві			Характер кіберзагроз
	$K_{\text{про}}$	G	$P_{\text{кнб}}$	
Стабільність на основі балансу сил та інтересів	≈ 0	≈ 1	≈ 0	Відсутність кіберзагрози
Стабільність на основі балансу інтересів	≈ 0	$\neq 1$	≈ 0	
Стабільність на основі балансу сил	< 1	≈ 1	До 0,25	Потенційна кіберзагроза
Відносна стабільність на основі пасивного відвернення	< 1	> 1		
Відносна стабільність на основі активного відвернення	> 1	<1	0,25÷0,85	Реальна кіберзагроза
Нестабільність на основі дисбалансу сил та інтересів	$> 1{,}5$	$> 1{,}5$	0,25÷0,85	Кіберзагроза
			>0,85	Безпосередня кіберзагроза

Висновки

Все викладене в статті, як і щоденне життя, переконливо доводить: забезпечення кібернетичної безпеки – процес безперервний, надзвичайно складний і багатогранний, причому успіх у його реалізації зумовлюється станом відносин у суспільстві і залежить від кожного його представника, але передусім від здійснення державної політики у цій сфері. Отримані результати достатньо чітко визначають критерій кібернебезпеки, який виходить із чисельних значень індексу кібернебезпеки або кіберзагрози. За допомогою цього критерію можна також уточнювати і рівні стабільності у суспільстві у випадках, коли сукупність значень величини $K_{\text{про}}$ і G.

Крім того розрахунок індексу кіберзагрози та визначення відповідного характеру кіберзагрози відповідного характеру кіберзагрози дає змогу шляхом рішення оберненої задачі зробити за допомогою табл. 1 впевнений висновок щодо рівня стабільності у суспільстві. Також є можливість визначити ймовірність порушення системи кіберзахисту, що дає змогу більш точно визначати кіберзагрози інформаційній системі держави.

Питання щодо критерія оцінки рівня кіберзагрози, то реакція організації протидії на кіберзагрозу різних рівнів відрізняється, перш за все, оперативністю та масштабами заходів, що здійснюється з метою досягнення бажаного рівня кібербезпеки, тобто рівня відбиття кібератаки.

Отже, критерій оцінки рівня кіберзагрози має опиратися головним чином, на характер кіберзагрози з обов'язковим урахуванням її масштабу. Обидва показники мають кількісний вимір, однак безпосереднє зведення їх до одного узагальненого показника не має підстав через принципову різницю між явищами, що ними характеризуються. Тому найбільш раціональним шляхом є логічний аналіз.

Таким чином, кожному рівню кіберзагрози відповідає свій рівень кібербезпеки. Отже, критерієм оцінки рівня кібербезпеки є рівень кіберзагрози.

Література

[1] Грищук Р.В. *Основи кібернетичної безпеки*/ Р.В. Грищук, Ю.Г. Даник. – Житомир: ЖНАЕУ, 2016. – 616 с.

[2] Бурячок В.Л. *Інформаційна та кібербезпека: соціотехнічний аспект* / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

[3] Хорошко В.О. Методичний підхід щодо оцінки рівня безпеки інформації / В.О. Хорошко, В.С. Чередниченко // *Зб. наук. праць ВІ КНУ ім. Тараса Шевченка*, Вип №14, 2008. – С. 176-181.

[4] Хорошко В.О. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко // *Інформаційні технології та комп'ютерна інженерія*, №3 (13), 2008. – С. 49-58.

[5] Дудикевич В.Б. *Основи інформаційної безпеки* / В.Б. Дудкевич, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця: ВНТУ, 2018. – 316 с.

[6] Тарасов В.А. *Интеллектуальные системы поддержки принятия решений: теория, синтез, эффективность* / В.А. Тарасов, Б.М. Герасимов, И.А. Левин, В.А. Корнейчук. – К.: МАКНС, 2007. – 336 с.

[7] Чалдин Р. *Психология влияния* / Р. Чалдин. – СПБ: Питер, 2016. – 336 с.

[8] Brailovskyi N. *Evaluation of the Level of Cyber Security of Information* / Brailovskyi N., Khoroshko V., Khokhlacheva Y., Ayasrah Ahmad // Scientific and Practical Cyber Security Journal (SPCSJ), vol3, #3, 2019. – pp. 18-24.

[9] Гришина Н.В. *Организация комплексной системы защиты информации* / Н.В. Гришина. – М: Гелиос АРВ, 2007. – 256 с.

УДК 004.056:351.862.4

Пискун И.В., Ткач Ю.Н., Хорошко В.А., Хохлачева Ю.Е., Аясрах А., Аль-Далваш А. Количественно-качественная оценка и определение уровня кибербезопасности информационных систем государства.

Аннотация. *В статье разработана методика количественно-качественного анализа и определения уровня кибербезопасности информационных систем государства. Обеспечение кибернетической безопасности - процесс непрерывный, чрезвычайно сложный и многогранный, причем успех в его реализации обусловлено состоянием отношений в обществе и зависит от каждого его представителя, но прежде всего от осуществления государственной политики в этой сфере. Полученные результаты достаточно четко определяют критерий кибернебезпекы, который выходит из численных значений индекса кибернебезпекы или киберугрозы. Критерий оценки уровня киберугрозы должна опираться на характер киберугрозы с обязательным учетом его масштаба. Оба показателя имеют количественное измерение, однако непосредственное сведение их к одному обобщенного показателя нет оснований из-за принципиальной разницы между явлениями, которыми характеризуются. Поэтому наиболее рациональным путем является логический анализ. Таким образом, в статье показано, что каждому уровню киберугрозы соответствует свой уровень кибербезопасности. Итак, критерием оценки уровня кибербезопасности является уровень киберугрозы.*

Ключевые слова: *кибербезопасность, уровень кибербезопасности, информационные системы государства, количественно-качественный анализ*

Piskun I.V, Tkach Y.M., Khoroshko V.O., Khokhlachova Y.E., Ayasrah A., Al-Dalvash A. Quantitative assessment and determination of the level of cyber security of state information systems.

Abstract. *The article develops a method of quantitative and qualitative analysis and determination of the level of cybersecurity of information systems of the state. Ensuring cyber security is a continuous, extremely complex and multifaceted process, and the success of its implementation is determined by the state of relations in society and depends on each of its representatives, but above all on the implementation of public policy in this area. The obtained results clearly define the criterion of cybersecurity, which is based on the numerical values of the index of cybersecurity or cyberthreat. The criterion for assessing the level of cyber threat should be based on the nature of the cyber threat, taking into account its scale. Both indicators have a quantitative dimension, but their direct reduction to one generalized indicator has no basis because of the fundamental difference between the phenomena characterized by them. Therefore, the most rational way is logical analysis. Thus, the article shows that each level of cyber threat corresponds to its own level of cybersecurity. Thus, the criterion for assessing the level of cybersecurity is the level of cyber threat.*

Keywords: *cybersecurity, level of cybersecurity, state information systems, quantitative and qualitative analysis*

Пискун Ігорь Васильович, науковий співробітник Національного авіаційного університету.
Пискун Игорь Васильевич, научный сотрудник Национального авиационного университета.
Pyskun Igor, researcher at the National Aviation University.

Ткач Юлія Миколаївна, д.пед.н., професор, завідувач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».
Ткач Юлия Николаевна, д.пед.н., профессор, заведующий кафедрой кибербезопасности и математического моделирования Национального университета «Черниговская политехника».
Tkach Yuliia, Doctor of Pedagogical Sciences, Professor, Head of the Department of Cybersecurity and Mathematical Simulation of the National University "Chernihiv Polytechnic".

Хорошко Володимир Олексійович, д.т.н., професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Хорошко Владимир Алексеевич, д.т.н., профессор, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Khoroshko Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Information Technology Security of the National Aviation University.

Хохлачова Юлія Євгеніївна, к.т.н., доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Хохлачева Юлия Евгеньевна, к.т.н., доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Khokhlachova Yulia, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Security of Information Technologies of the National Aviation University.

Аясрах Ахмад Расмі Алі, аспірант, Національний авіаційний університет.
Аясрах Ахмад Расми Али, аспирант, Национальный авиационный университет.
Ayasrah Ahmad Rasmi Ali, graduate student, National Aviation University.

Аль-Далваш Аблуллах Фоуад, аспірант, Національний авіаційний університет.
Аль-Далваш Аблуллах Фоуад, аспирант, Национальный авиационный университет.
Al-Dalvash Ablullah Fowad, graduate student, National Aviation University.

Отримано *26 листопада 2020 року*, затверджено редколегією *15 грудня 2020 року*