ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.9.056.5:510.644.4 **doi: 10.32620/reks.2020.4.10**

І. В. ШЕЛЕХОВ[1,2], Н. Л. БАРЧЕНКО[1], В. В. КАЛЬЧЕНКО[2,3], В. К. ОБОДЯК[1]

[1] ***Сумський державний університет, Україна***
[2] ***Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна***
[3] ***Управління Держспецзв'язку в Сумській області, Україна***

НЕЧІТКА ІЄРАРХІЧНА ОЦІНКА ЯКОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Зміни в законодавстві України призводять до поступового переходу на міжнародні стандарти в сфері забезпечення захисту інформації в інформаційно-комунікаційних системах державних органів і об'єктів критичного призначення. Але оскільки новітня нормативна база в основному створюється на базі нормативних документів минулих років, то виникає необхідність розроблення нових підходів до оцінки захищеності інформаційно-комунікаційних систем. Одним із варіантів вирішення даної проблеми є застосування методів тестування на проникнення та апарату нечіткої логіки. Під час даної процедури відбувається тестування параметрів комплексу засобів захисту за допомогою загальнодоступних інструментів, які використовуються і зловмисниками. Після завершення даної процедури можливі три варіанти результатів, які описуються нечіткими термами: система відповідає вимогам нормативних документів, система не відповідає вимогам нормативних документів, система частково відповідає вимогам нормативних документів та потребує доопрацювання. Внаслідок цього постає завдання розробки моделі, яка б дозволяла на основі нечіткої бази знань отримати інтегральний показник захищеності. В статті проведений аналіз міжнародних документів в сфері кібербезпеки та нормативної документації системи технічного захисту інформації України. Для оцінки інформаційно-комунікаційної системи були вибрані критерії захищеності від несанкціонованого доступу, які визначені в існуючих національних нормативних документах. Розроблена модель нечіткої ієрархічної системи оцінювання профілю захищеності, яка задає множину критеріїв оцінювання та послідовність їх використання. Запропонована ієрархічна модель дозволяє подати процес оцінювання у явному виді та реалізувати процес перевірки критеріїв із зазначенням ступеню впевненості експерта у релевантності критеріїв оцінювання. Система була реалізована у середовищі Fuzzy Logic Toolbox пакету прикладних програм Matlab. Проведені комп'ютерні експерименти показали можливість застосування розробленої моделі на практиці.

Ключові слова: *кібербезпека; критерії захищеності; нечітка логіка; профіль захищеності.*

Вступ

Протягом останніх років у законодавстві України відбулись зміни, пов'язані із захистом інформації в інформаційно-комунікаційних системах (ІКС) та кіберзахистом об'єктів критичної інфраструктури:

- згідно з Законом України [1] було дозволено обробку державних інформаційних ресурсів та інформації з обмеженим доступом (крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами) без застосування комплексної системи захисту інформації (КСЗІ). Зазначеним законом дозволено використовувати міжнародний підхід в сфері забезпечення захисту інформації.
- згідно з Законом України [2] єдиним методом кіберзахисту об'єктів критичної інфраструктури та систем, де обробляється державна таємниця та службова інформація, є побудова КСЗІ.

Таким чином, з одного боку здійснюється поступовий перехід на західний варіант забезпечення захисту інформації, а з іншого боку в нових нормативних документах залишається вимога щодо використання КСЗІ як методу забезпечення захисту інформації.

Проте, незважаючи на зміни законодавства, удосконалення існуючої системи побудови КСЗІ в інформаційно-телекомунікаційних системах державних органів щодо процедури оцінки вжитих заходів із захисту та її подальшої оцінки після введення в експлуатацію не в повній мірі відповідає сучасним вимогам. Тому на даний момент гостро стоїть питання удосконалення порядку оцінки систем захисту як на підставі міжнародного досвіду так і з врахуванням існуючої нормативно-правової бази. При цьому основним шляхом розв'язання цієї важливої задачі є застосування ідей і методів інтелектуального аналізу даних.

Аналіз публікацій

Розглядаючи методи оцінки інформаційно-комунікаційних систем, варто зазначити що існує декілька підходів до оцінювання: експертна оцінка, кількісна оцінка, змішаний підхід (CRAMM, RiskWatch) та підхід заснований на нормативних документах [3]. Аналізуючи роботи українських науковців варто зазначити, що вони будуються на основі експертної оцінки деяких критеріїв.

В [4] було запропоновано використовувати метод аналізу ієрархій та апарату нейронно-нечітких мереж для оцінки захищеності системи, проте дана модель не має прив'язки до існуючої нормативної бази України.

В [5] пропонується проводити оцінку методом експертного оцінювання захищеності систем, а в якості критеріїв використовувати, як вітчизняні нормативні документи так і нормативні документи США. Але автори не зазначають, яким чином експерти будуть отримувати відповідну оцінки.

В [6] запропоновано кількісно оцінювати цільову систему виходячи з вартості інформації що захищається, ймовірності злому, продуктивності системи і т.д. Проте при цьому виникають проблеми адекватної оцінки зазначених критеріїв. В [7] достатньо повно описані ключові фактори, які впливають на захищеність інформації, але дана модель оперує такими критеріями, як захист інформації від витоку технічними каналами, розголошення інформації персоналом, організаційне забезпечення захисту інформації які, як правило відсутні, в технічному завданні на створення системи захисту інформації.

Найбільш розповсюдженим міжнародним варіантом оцінки системи захисту інформації для складних ІКС є застосування стандарту ISO/IEC 15408. Положення зазначеного стандарту використовують для оцінки захищеності інформаційної системи з точки зору повноти реалізованих в ній функцій безпеки і надійності реалізації цих функцій.

Проте незважаючи на різні підходи до оцінювання захищеності ІКС, варто констатувати, що кожен день фахівці в сфері кібербезпеки знаходять нові вразливості в програмному забезпеченні комп'ютерних систем. Згідно національної бази даних вразливостей Національного інституту стандартів та технологій США в період з вересня по листопад 2020 року було виявлено близько 5400 таких вразливостей [8]. Тому навіть при якісному врахуванні всіх сучасних загроз, виборі програмних (апаратних) засобів захисту, їх коректного налаштуванні, на момент завершення процедури оцінки, система захисту з великою вірогідністю буде мати деякі вразливості.

У зв'язку зі стрімким розвитком способів, методів і інструментарію отримання несанкціонованого доступу до інформаційних систем, необхідно використовувати методи оцінки, які б: з одного боку дозволяли оцінити реальний стан захищеності ІКС, а з іншого боку дозволяли підтвердити або спростувати відповідність системи захисту ІКС вимогам національного законодавства.

Аналізуючи досвід інших країн, варто зупинитись на такому методі оцінювання, як тестування на проникнення (penetration test).

Тестування на проникнення – це метод оцінювання захищеності ІКС, шляхом моделювання дій зловмисників для отримання доступу до конфіденційної інформації, що в ній циркулює, порушення її цілісності або доступності. Якісно проведене тестування дозволяє визначити рівні захищеності ІКС та наявності в ній вразливостей, ідентифікувати найбільш вірогідні шляхи порушення встановленої політики безпеки і визначити наскільки якісно працює комплекс засобів захисту такої системи [9].

Зазначений метод оцінювання захищеності впроваджений як в національні нормативні документи різних країн світу, так і в міжнародні стандарти. Наприклад, в Сполучених штатах Америки прийнятий документ [10] згідно якого, при оцінці ефективності захищеності федеральних інформаційних систем повинно застосовуватись тестування на проникнення.

В Федеративній республіці Німеччина розроблено і впроваджено методологію визначення та впровадження заходів з комп'ютерної безпеки в федеральних органах влади (German: IT-Grundschutz). Згідно з концепцією IT-Grundschutz, Німецьке федеральне управління з питань інформаційної безпеки (BSI) розробило перелік стандартів та надає рекомендації щодо оцінки стану захисту інформації.

В стандарті BSI-Standard 200-1 Information Security Management Systems (ISMS) при виборі засобів безпеки вимагається використовувати тести на проникнення для практичної перевірки реалізації встановлених заходів з захисту [11]. В свою чергу, міжнародні стандарти ISO 17799, ISO 27001, стандарт безпеки індустрії платіжних карт PCI DSS також вимагають проведення тестування на проникнення [12].

Аналізуючи статті українських вчених, варто зазначити що в статтях [13, 14] пропонувалось використовувати тестування на проникнення, як метод перевірки захищеності складних ІКС. Але в них не було запропоновано підходів, які б дозволили поєднати даний вид тестування з існуючою українською нормативною базою.

Аналізуючи українське законодавство, варто зазначити, що обов'язковість проведення тестування на проникнення визначено документом [15] лише для банківської сфери. На момент написання даної статті,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

для українських державних ІКС, обов'язковість проведення такої процедури нормативно не закріплена.

Варто зазначити, що відповідно до документу [16] планове оцінювання захищеності методом тестування на проникнення повинно здійснюватися не менше одного разу на п'ять років. Проте через обмежену кількість фахівців відповідне оцінювання проводиться лише в деяких державних органах і вкрай рідко. Крім того, в вільному доступі відсутні будь-які методики, інструкції, тощо, які регламентують проведення процедури тестування на проникнення.

Основним документом, який регламентує оцінювання захищеності ІКС державних органів є Положення про державну експертизу в сфері технічного захисту інформації [17]. Зазначений документ встановлює загальні вимоги до процесу проведення державної експертизи, розподілення обов'язків між суб'єктами взаємовідносин, строки дії дозвільних документів, тощо.

В "Методичних вказівках з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу", затверджених наказом Адміністрації Держспецзв'язку від 24.07.2009 №172 зі змінами внесеними наказом від 28.12.2012 №806 (НД ТЗІ 2.7-009-09) безпосередньо описано процедуру проведення об'єкта експертизи, а саме засобів захисту інформації в комп'ютерних системах від несанкціонованого доступу та комплексів засобів захисту КСЗІ в ІКС.

Згідно пункту 5.1.5 нормативного документу НД ТЗІ 2.7-009-09 методологія оцінювання функцій захисту передбачає 5 основних етапів робіт: попередній аналіз оцінюваного об'єкту експертизи, розроблення програми випробувань функціональних послуг безпеки, розроблення методики випробувань функціональних послуг безпеки, проведення випробувань, аналіз, документування та затвердження результатів випробувань. Основним недоліком даних етапів є те, що вони будуються на документації, яку пред'являє замовник.

Якщо розглядати етап попереднього аналізу оцінюваного об'єкту експертизи, то такий підхід є виправданим. Проте при розробленні програми та методики потрібно згідно з розділом 5.3 НД ТЗІ 2.7-009-09 також використовувати документацію надану розробником об'єкта експертизи і тільки її, що робить підхід до оцінювання однобоким та суб'єктивним. Це пов'язано з тим, що розробник зацікавлений в отриманні експертного висновку, так як це дозволить отримати грошові кошти за побудову КСЗІ.

Отже, ми маємо концептуальні проблеми в оцінюванні захищеності ІКС, які підключені до мережі Інтернет. Можливим варіантом вирішення даної проблеми є розробка математичної моделі, яка дозволить при використанні методу тестування на проникнення з одного боку отримати деякий числовий коефіцієнт ступеню захищеності ІКС, а з іншого підтвердити або спростувати реалізацію профілю захищеності, що був визначний на етапі розробки системи захисту інформації.

Постановка завдання

Метою даної статті є розробка моделі оцінювання захищеності ІКС державних органів з використанням методів тестування на проникнення та апарату нечіткої логіки для отримання висновка щодо стану захищеності цільової інформаційної, комунікаційної системи.

Для досягнення поставленої мети необхідно вирішити наступні завдання.

1. Виконати математичний опис завдання оцінювання захищеності ІКС.
2. Розробити модель системи нечіткого логічного виведення.
3. Розглянути приклад застосування розробленої моделі.

Математичний опис завдання оцінки захищеності ІКС

Проведений аналіз нормативних документів технічного захисту інформації (НД ТЗІ 2.5-004-99, НД ТЗІ 2.7-009-09) надав можливість подати системи критеріїв оцінки захищеності ІКС структурою:

$$S = < M \times R \times P >, \quad (1)$$

де M – множина критеріїв;

R – множина відношень (зв'язків) між критеріями;

P – множина складових (елементів) критеріїв або підкритеріїв.

При цьому, множина R встановлює послідовність застосування критеріїв M або підкритеріїв P і дозволяє створити їх ієрархію. Наприклад, аналіз НД ТЗІ 2.5-004-99 надав можливість подати систему критеріїв оцінки профілю захисту (ПЗ) структурою:

$$M = < X, Y, V, B, W, E >, \quad (2)$$

де X – множина критеріїв конфіденційності;

Y – множина критеріїв цілісності;

V – множина критеріїв доступності;

B – множина критеріїв спостережуваності;

W – множина критеріїв гарантії;

E – інтегральний показник відповідності ПЗ вимогам.

При цьому

$$X = < \{x_i, Valx_i\} \Big| i \in (\overline{1,5}) >, \quad (3)$$

де x_i – множина критеріїв оцінки конфіденційності (x_1 – довірча конфіденційність, x_2 – адміністративна конфіденційність, x_3 – повторне використання об'єктів, x_4 – аналіз прихованих каналів, x_5 – конфіденційність при обміні);

$Valx_i$ – допустимі значення критеріїв оцінки конфіденційності.

Крім того,

$$Y = < \{y_i, Valy_i\} \Big| i \in (\overline{1,4}) >, \quad (4)$$

де y_i – множина критеріїв оцінки цілісності (y_1 – довірча цілісність, y_2 – адміністративна цілісність, y_3 –відкат, y_4 – цілісність при обміні);

$Valy_i$ – допустимі значення критеріїв оцінки цілісності;

$$V = < \{v_i, Valv_i\} \Big| i \in (\overline{1,4}) >, \quad (5)$$

де v_i – множина критеріїв оцінки доступності (v_1 – використання ресурсів, v_2 – стійкість до відмов, v_3 – гаряча заміна, v_4 – відновлення);

$Valv_i$ – допустимі значення критеріїв оцінки доступності;

$$B = < \{b_i, Valb_i\} \Big| i \in (\overline{1,9}) >, \quad (6)$$

де b_i – множина критеріїв оцінки спостереженості (b_1 – реєстрація, b_2 – ідентифікація, b_3 – достовірний канал, b_4 – розподіл обов'язків, b_5 – цілісність комплекту засобів захисту, b_6 – самотестування, b_7 – ідентифікація при обміні, b_8 – автентифікація відправника, b_9 – автентифікація отримувача);

$Valb_i$ – допустимі значення критеріїв оцінки спостереженості;

$$W = < \{w_i, Valw_i\} \Big| i \in (\overline{1,7}) >, \quad (7)$$

де bw_i – множина критеріїв гарантії,

$Valb_i$ – допустимі значення критеріїв гарантії;

$$E \in \{e_1, e_2, e_3\},$$

де e_1 = «не відповідає»,

e_2 = «частково відповідає»,

e_3 = «відповідає».

У кожному конкретному випадку критерії відбираються на підставі аналізу моделі загроз, моделі порушника, політики безпеки та зазначаються в технічному завданні на створення КСЗІ.

Модель нечіткого логічного виведення

Оцінювання ПЗ відноситься до задачі класифікації, яка може бути розв'язана за допомогою методів інтелектуального аналізу даних у тому числі методів, побудованих на основі машинного навчання та розпізнавання образів. Оскільки при оцінюванні використовується якісна шкала виміру, то одним із перспективних підходів до вирішення цієї задачі є застосування ієрархічної структури критеріїв оцінювання та методів логічного виведення для нечітких ієрархічних систем [18, 19]. У рамках цих методів загальна схема розв'язання задачі оцінювання ПЗ складається з таких дій:

а) фазифікація результатів перевірки необхідних умов та тестувань на проникнення;

б) процедура нечіткого логічного виведення послідовно для кожного рівня ієрархії;

в) оцінка критеріїв за принципом термометра [18];

г) дефазифікація результатів оцінювання.

При фазифікації використовуються нечіткі терм-множини, функції належності яких подані у вигляді трикутних L-R функцій (рис. 1). Наприклад, для *i*-того критерію оцінки конфіденційності x_i

$$\mu(x_i) = \begin{cases} 0, & \text{якщо } \left(x_i < Valx_{i,j-1}\right) \text{або } \left(x_i > Valx_{i,j+1}\right); \\ \dfrac{x_i - Valx_{i,j-1}}{Valx_{i,j} - Valx_{i,j-1}}, & \text{якщо } Valx_{i,j-1} \ge x_i \ge Valx_{i,j}; \\ \dfrac{Valx_{i,j+1} - x_i}{Valx_{i,j+1} - Valx_{i,j}}, & \text{якщо } Valx_{i,j} \ge x_i \ge Valx_{i,j+1}; \end{cases}$$

де $Valx_{i,j}$ – j-й рівень захищеності і-го критерію оцінки конфіденційності. При цьому для крайньої правої терм-множини $Valx_{i,j+1} = Valx_{i,j}$, а для крайньої лівої терм-множини $Valx_{i,j-1} = Valx_{i,j}$.

Ієрархію критеріїв оцінки подано на рис. 2 у вигляді дерева логічного виведення. Перевірка за кожним критерієм виконується на певному рівні ієрархії визначеною множиною R в залежності від того, результати перевірки яких критеріїв складають необхідну умову його обчислення.

При цьому множина підкритерів P складається з умов, що перевіряються при обчисленні певного критерію і не впливають на інші критерії оцінки. Нечіткі множини сформовані за результатом перевірки кри-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

теріїв відповідності визначеним для них рівням захищеності на верхніх рівнях ієрархії є вхідними даними для критеріїв нижніх рівнів. Таким чином, ієрархії відповідає система нечітких співвідношень

$$\tilde{C}_{k,i} = f\left(\left\{R\left(\tilde{C}_{k,i}\right)\right\};\left\{P\left(\tilde{C}_{k,i}\right)\right\}\right), \qquad (8)$$

де $\tilde{C}_{k,i}$ – і-й критерій, що обчислюється на k-му рівні ієрархії,

$\left\{R\left(\tilde{C}_{k,i}\right)\right\}$ – множина критеріїв, що входять в необхідну умову його обчислення,

$\left\{P\left(\tilde{C}_{k,i}\right)\right\}$ – множина його підкритеріїв.

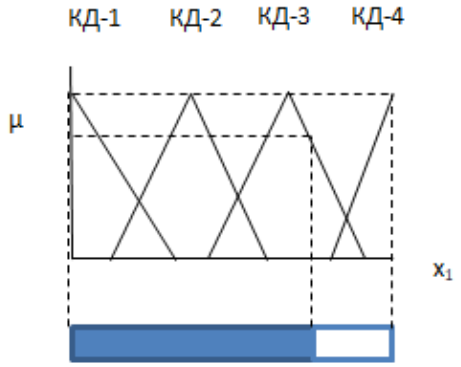

Рис. 1. Оцінювання змінної за принципом термометра

Нечіткі логічні рівняння дозволяють оцінювати інтегральний показник Е для фіксованих значень локальних показників. На першому кроці відбувається нечітке виведення для проміжних вершин локальних показників. На другому кроці чіткі значення цих змінних передаються в нечітку систему наступного рівня ієрархії.

Алгоритм нечіткого логічного виведення [15] має такий вигляд.

1. Фіксується вектор значень вхідних змінних.

2. Визначається значення функцій належності термів-оцінок вхідних змінних.

3. Обчислюються функції належності термів-оцінок вихідної величини, яка відповідає вектору значень вхідних змінних.

4. Визначається оцінка, функція належності якої максимальна.

Лінгвістичні змінні X, Y, V, B, W, E оцінюються нечіткими термами Нв – не відповідає, Чв – частково відповідає, Вв – відповідає.

Система продукційних правил має вигляд:

ЯКЩО (X=Вв) **ТА** (Y=Вв) **ТА** (V=Вв) **ТА** (B=Вв) **ТА** (W=Вв) **ТОДІ** E=Вв.

ЯКЩО (X=Нв) **АБО** (Y=Нв) **АБО** (V=Нв) **АБО** (B= Нв) **АБО ТОДІ** E= Нв.

ЯКЩО (X=Чв) **АБО** (Y=Чв) **АБО** (V=Чв) **АБО** (B=Чв) **АБО ТОДІ** E=Чв.

Обчислення вихідного значення відбувається за максимумом функції належності:

$$k^* = \arg\left(\max_k \mu\left(E_k\right)\right),$$

де k – номер правила,

$\mu(E_k)$ – ступінь виконання правила.

Приклад застосування розробленої моделі

Існує певна взаємопов'язана сукупність послуг безпеки, які повинні реалізовуватись будь-якою системою захисту. До них відносяться наступні послуги: цілісність комплексу захисту (НЦ-1), зовнішній аналіз (НР-1), виділення адміністратора (НО-1), зовнішня ідентифікація і автентифікація (НИ-1).

Для процедури оцінювання вибираємо ті критерії, які зазначені в технічному завданні. Вхідні дані після проведення експертних перевірок (тестування на проникнення, перевірка документації тощо) оцінюємо за принципом термометра.

Послуги, які перевірять тестуванням на проникнення: довірча конфіденційність (КД), адміністративна конфіденційність (КА), повторне використання об'єктів (КО), аналіз прихованих каналів (КК), конфіденційність при обміні (КВ), довірча цілісність (ЦД), мінімальна адміністративна цілісність (ЦА), мінімальна цілісність при обміні (ЦВ), стійкість до відмов(ДС), реєстрація (НР), ідентифікація і автентифікація (НИ), розподіл обов'язків (НО), цілісність КЗЗ (НЦ), ідентифікація і автентифікація при обміні (НВ), автентифікація відправника (НА), автентифікація отримувача (НП).

Послуги, які перевіряються іншими методами: відкат (ЦО), використання ресурсів (ДР), модернізація (ДЗ), відновлення після збоїв (ДВ), достовірний канал (НК), самотестування (НТ).

Нехай для оцінки наданий профіль {КД-2, КА-2, КО-1, КК-1, КВ-1, ЦД-1, ЦА-2, ЦО-1, ЦВ-1, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-2, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1, НА-1, НП-1}.

Необхідно оцінити те, наскільки повно комплекс засобів захисту його реалізує. Як приклад на рис. 3 наведено фрагмент опитування експерта щодо оцінювання множини критеріїв конфіденційності X та обчислення загальної оцінки.

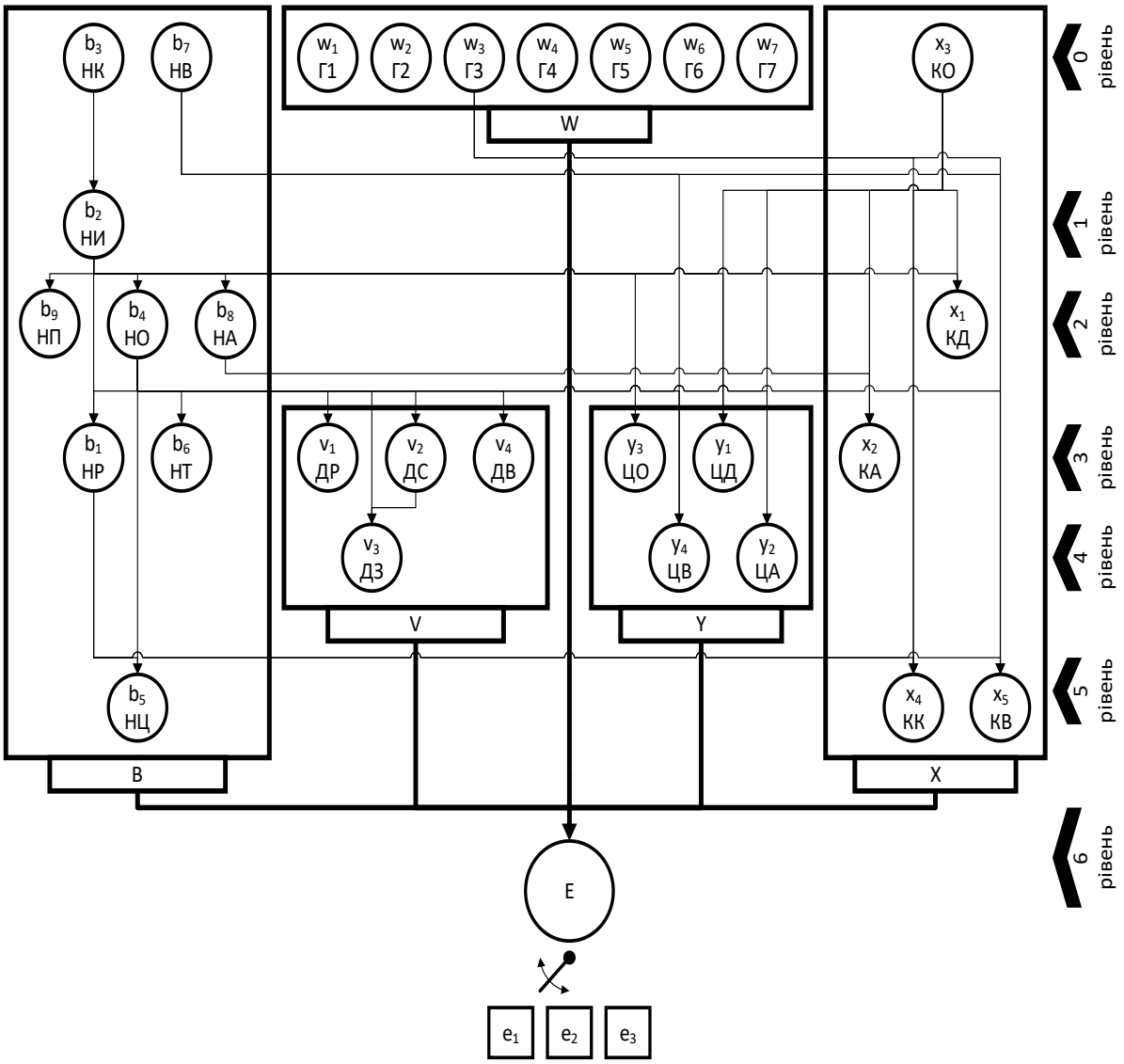

Рис. 2. Схема локальних та інтегрального показників

Рис. 3. Оцінка вхідних даних (фрагмент вікна)

Підсумкове значення X визначається як перетин нечітких значень x_1, x_2, x_3, x_4, x_5, яке потім передається на вхід нечіткої системи логічного виведення типу Мамдані.

Моделювання інтегрального показника E проведено у середовищі Fuzzy Logic Toolbox пакету Matlab (рис. 4).

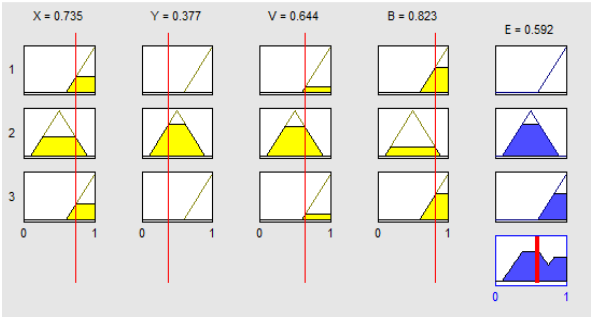

Рис. 4. Правила нечіткого виведення

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Отримана нечітка система дозволяє проводити моделювання оцінювання інтегрального показника E за різними значеннями входів X, Y, V, B.

Отримана оцінка E (рис. 4, 5) свідчить про часткову відповідність вимогам.

Змінна	Оцінка за принципом термометра
X	
x_1 (КД)	
x_2 (КА)	
x_3 (КО)	
x_4 (КК)	
x_5 (КВ)	
Y	
y_1 (ЦД)	
y_2 (ЦА)	
y_3 (ЦО)	
y_4 (ЦВ)	
V	
v_1 (ДР)	
v_2 (ДС)	
v_3 (ДЗ)	
v_4 (ДВ)	
B	
b_1 (НР)	
b_2 (НИ)	
b_3 (НК)	
b_4 (НО)	
b_5 (НЦ)	
b_6 (НТ)	
b_7 (НВ)	
b_8 (НА)	
b_9 (НП)	
Інтегральна оцінка	
E	Частково відповідає

Рис. 5. Результат оцінювання

Висновки

Був проведений математичний опис завдання оцінювання захищеності ІКС. Система критеріїв оцінки задана ієрархічною структурою, яка містить інформацію щодо критеріїв, відношень між ними та множини складових елементів критеріїв на прикладі НД ТЗІ 2.5-004-99.

Ієрархію критеріїв оцінки подано у вигляді дерева логічного виведення. Перевірка за кожним критерієм виконується на певному рівні ієрархії визначеною множиною *R* в залежності від того, результати перевірки яких критеріїв складають необхідну умову його обчислення. Розроблена структура являє собою нечітку мережеву модель, яка містить знання о зв'язках між критеріями та нечіткі знання щодо їх суб'єктивних оцінок, що надаються експертами.

Розроблена система нечіткого логічного виведення для оцінки інтегрального показника відповідності та наведений приклад її реалізації в Fuzzy Logic пакету Matlab.

Удосконалено нечітку модель шляхом введення ієрархічної структури критеріїв оцінювання, що дозволило подати процес оцінювання у явному виді та реалізувати процес перевірки критеріїв із зазначенням ступеню впевненості експерта у релевантності критеріїв оцінювання.

Практична значимість полягає в тому, що розроблена модель дозволяє удосконалити та частково автоматизувати процес оцінювання.

Подальші дослідження будуть спрямовані на аналіз можливості інтеграції різних алгоритмів навчання до розробленої моделі.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України № 80/94-ВР, редакція від 04.07.2020 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text – 26.08.2020.

2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518-2019-п [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text – 26.08.2020.

3. Юдін, О. Підходи до оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних системах на стадії модернізації [Текст] : моногр. / О. К. Юдін, М. А. Стрельбіцький ; под общей редакцией В. М. Безрука, В. В. Баранника // Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба. – Х. : Издательство «Лидер», 2017. – С. 582– 599.

4. Климович, О. Методичні основи оцінки контролю захищеності інформаційно-телекомунікаційної мережі спеціального призначення [Електронний ресурс] / О. К Климович // Теоретичні основи розробки та експлуатації систем озброєння. – 2018. – Т. 1, № 53. – С. 143–147. DOI: 10.30748/soivt.2018.53.20.

5. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку [Текст] / В. В. Куцаєв [та ін.] // Збірник наукових праць ВІТІ. – 2018. – Т. 2. – С. 67–76.

6. Крайнов, О. В. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління [Текст] / О. В. Крайнов, М. Ф. Маланчук, Р. І. Грозовський // Modern Information Technologies in the Sphere of Security and Defence. – 2020. – Т. 37, № 1. – С. 103-106. DOI: 10.33099/2311-7249/2020-37-1-103-106.

7. Салієва, О. В. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання [Текст] / О. В. Салієва, Ю. Є. Яремчук // Безпека інформації. – 2020. – Т. 26, № 1. – С. 42-49. DOI: 10.18372/2225-5036.26.14669.

8. Search Vulnerability Database [Електронний ресурс]. – Режим доступу: https://nvd.nist.gov/vuln/search. – 26.08.2020.

9. The Penetration Testing Framework for Large-scale Network Based on Network Fingerprint [Text] / Pengfei Shi at al. // Information System and Computer Engineering (CISCE), 2019. – P. 378–381. DOI: 10.1109/CISCE.2019.00089.

10. NIST Special Publication 800-53A. Revision 4. Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Building Effective Assessment Plans [Електронний ресурс]. – Режим доступу: https://doi.org/10.6028/NIST.SP.800-53Ar4 – 26.11.2020 р.

11. BSI Standard 200-1. Information Security Management Systems (ISMS) [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=3 – 26.08.2020.

12. Requirements and Security Assessment Procedures [Електронний ресурс]. – Effective from 2018-05-01. – Official edition. – [S. l. : s. n.], 2018. – 139 p. – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1606415382301 – 26.08.2020.

13. Бурячок, В. Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах [Текст] / В. Л. Бурячок // Сучасний захист інформації. – Київ, 2015. – № 3. – С. 4–12.

14. Киричок, Р. В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення [Текст] / Р. В Киричок и др. // Наукові записки Українського науково-дослідного інституту зв'язку. – Київ, 2016. – № 3(43). – С. 48–61.

15. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Національного банку України від 28.09.2017 р. № 95 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17#n12 – 26.08.2020.

16. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Наказ від 02.12.2014 р. № 660 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0090-15#Text – 26.08.2020.

17. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації: Наказ від 16.05.2007 р. № 93 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07#Text – 26.08.2020.

18. Роштейн, О. Моделювання та оптимізація надійності багатовимірних алгоритмічних процесів [Текст] / О. П. Роштейн, С. Д. Штовба, О. М. Козачко. – Вінниця : УНІВЕРСУМ-Вінниця, 2007. – 212 с.

19. Organizational Approach to the Ergonomic Examination of E-Learning Modules [Text] / E. Lavrov, O. Kupenko, T. Lavryk, N. Barchenko // Informatics in education. – 2013. – No. 12(1). – P. 107–124. DOI: 10.15388/infedu.013.08.

References

1. *Law of Ukraine. On information protection in information and telecommunication systems, No. 80/94-BP, Revision on July 4, 2020*. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (accessed 26.08.2020).

2. *Resolution of the Cabinet of Ministers of Ukraine. On approval of the General requirements for cyber protection of critical infrastructure No. 518-2019-n, Adoption on June 19, 2019*. Available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (accessed 26.08.2020).

3. Yudin, O., Strel'bits'kyy, M. Pidkhody do otsinyuvannya efektyvnosti zakhystu informatsiyi v informatsiyno-telekomunikatsiynykh systemakh na stadiyi modernizatsiyi [Approaches to evaluating the effectiveness of information protection in information and telecommunication systems at the stage of modernization]. *Naukoemkye tekhnolohyy v ynfo-kommunykatsyyakh: obrabotka ynformatsyy, kyberbezopasnost', ynformatsyonnaya bor'ba*, Kharkiv, Lider Publ., 2017, pp. 582-599.

4. Klymovych, O. Metodychni osnovy otsinky kontrolyu zakhyshchenosti informatsiyno-telekomunikatsiynoyi merezhi cpetsial'noho pryznachennya [Methodical bases of an estimation of control of protection of an information and telecommunication network of a special purpose]. *Teoretychni osnovy rozrobky ta ekspluatatsiyi system ozbroyennya*, 2018, vol. 1, no. 53, pp. 143-147. DOI: 10.30748/soivt.2018.53.20.

5. Kutsayev, V. V. at al. Metodyka otsinky kibernetychnoyi zakhyshchenosti informatsiyno-telekomunikatsiynoho vuzla zv"yazku [Methods for assessing the cyber security of information and telecommunications nodes]. *Zbirnyk naukovykh prats' VITI*, 2018, vol. 2, pp. 67-76.

6. Kraynov, O. V., Malanchuk, M. F., Hrozovs'kyy, R. I. Metodyka otsinky efektyvnosti kompleksnoyi systemy zakhystu informatsiyi avtomatyzovanykh informatsiynykh system orhaniv viys'kovoho upravlinnya [Methods for assessing the effectiveness of a comprehensive system of information protection of automated information systems of military authorities]. *Modern Information Technologies in the Sphere of Security and Defence*, 2020, vol. 37, no. 1, pp. 103-106. DOI: 10.33099/2311-7249/2020-37-1-103-106.

7. Saliieva, O., Yaremchuk, Yu. Vyznachennya rivnya zakhyshchenosti systemy zakhystu informatsiyi na osnovi kohnityvnoho modelyuvannya [Determining the level of security of the information security system based on cognitive modeling]. *Bezpeka ìnformacìì – Ukrainian Scientific Journal of Information Security,*

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

2020, vol. 26, no. 1, pp. 42-49. DOI: 10.18372/2225-5036.26.14669.

8. *Search Vulnerability Database* [online]. Available at: https://nvd.nist.gov/vuln/search (accessed 26.08.2020).

9. Shi, Pengfei. at al. The Penetration Testing Framework for Large-scale Network Based on Network Fingerprint. *Information System and Computer Engineering (CISCE)*, 2019, pp. 378–381. DOI: 10.1109/CISCE.2019.00089.

10. *NIST Special Publication 800-53A. Revision 4. Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Building Effective Assessment Plans.* Available at: https://doi.org/10.6028/NIST.SP.800-53Ar4 (accessed 26.08.2020).

11. *BSI Standard 200-1. Federal Office for Information Security. Information Security Management Systems (ISMS)*. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.pdf?__blob=publicationFile&v=3 (accessed 26.08.2020).

12. PCI Security Standards Council. Requirements and Security Assessment Procedures. Available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1606415382301 (accessed 26.08.2020).

13. Buryachok, V., Kozachok, V., Buryachok, L. and Skladannyy, P. Pentestinh yak instrument kompleksnoyi otsinky efektyvnosti zakhystu informatsiyi v rozpodilenykh korporatyvnykh merezhakh [Pentesting as a tool for comprehensive assessment of the effectiveness of information security in distributed corporate networks]. *Suchasnyy zakhyst informatsiyi*, 2015, vol. 3, pp. 4–12.

14. Kyrychok, R., Skladannyy, P., Buryachok, V., Hulak, H. and Kozachok, V. Problemy zabezpechennya kontrolyu zakhyshchenosti korporatyvnykh merezh ta shlyakhy yikh vyrishennya [Problems of ensuring security control of corporate networks and ways to solve them] *Naukovi zapysky Ukrayins'koho naukovo-doslidnoho instytutu zv"yazku*, 2016, vol. 3, no. 43, pp. 48–61.

15. *Resolution of the National Bank of Ukraine. On approval of the Regulations on the organization of measures to ensure information security in the banking system of Ukraine*, No. 95, 28 September 2017. Available at: https://zakon.rada.gov.ua/laws/show/v0095500-17#n12 (accessed 26.08.2020).

16. *Order of State Service of Special Communication and Information Protection of Ukraine. About the statement of the Procedure for an assessment of a condition of protection of the state information resources in information, telecommunication and information-telecommunication systems*, No. 660, 2 December 2014. Available at: https://zakon.rada.gov.ua/laws/show/z0090-15#Text (accessed 26.08.2020).

17. *Order of State Service of Special Communication and Information Protection of Ukraine. On approval of the Regulations on state expertise in the field of technical protection of information*, No. 93, 16 May 2007. Available at: https://zakon.rada.gov.ua/laws/show/z0820-07#Text (accessed 26.08.2020).

18. Rotshteyn, O., Shtovba, S. and Kozachko, O. *Modelyuvannya ta optymizatsiya nadiynosti bahatovymirnykh alhorytmichnykh protsesiv* [Modeling and optimization of reliability of multidimensional algorithmic processes]. Vinnytsia, UNIVERSUM-Vinnytsya, 2007. 212 p.

19. Lavrov, E., Kupenko, O., Lavryk, T., Barchenko, N. Organizational Approach to the Ergonomic Examination of E-Learning Modules. *Informatics in education*, 2013, vol. 12, no. 1, pp. 107-124. DOI: 10.15388/infedu.013.08

Поступила в редакцию 15.09.2020, рассмотрена на редколлегии 16.11.2020

НЕЧЕТКАЯ ИЕРАРХИЧЕСКАЯ ОЦЕНКА КАЧЕСТВА КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

І. В. Шелехов, Н. Л. Барченко, В. В. Кальченко, В. К. Ободяк

Изменения в законодательстве Украины приводят к постепенному переходу на международные стандарты в области обеспечения защиты информации в информационных, коммуникационных системах государственных органов. Однако новейшая нормативная база опирается на нормативные документы прошлых лет. В связи с этим возникла необходимость разработать новые подходы в оценке защищенности информационных, коммуникационных системах. Одним из вариантов решения данной проблемы является применение методов тестирования на проникновение. Во время данной процедуры происходит тестирование параметров комплекса средств защиты с помощью общедоступных инструментов, используемых злоумышленниками. После завершения данной процедуры возможны три варианта результатов, которые описываются нечеткими термами: система соответствует требованиям нормативных документов, система не соответствует требованиям нормативных документов, система частично соответствует требованиям нормативных документов и нуждается в доработке. В результате возникает задача разработки модели, позволяющей на основе нечеткой базы знаний получить интегральный показатель защищенности. В статье проведен анализ международных документов в сфере кибербезопасности и нормативной документации системы технической защиты информации Украины. В качестве критериев оценки системы были выбраны критерии защищенности от несанкционированного доступа, которые определены в существующих национальных нормативных документах. Разработана модель нечеткой иерархической системы оценки профиля защищенности, которая задает множество критериев оценки и последовательность их использования. Предложенная иерархическая модель позволяет представить процесс оценивания в явном виде и реализовать процесс проверки критериев с указанием степени

уверенности эксперта в релевантности критериев оценки. Система была реализована в среде Fuzzy Logic Toolbox пакета прикладных программ Matlab. Проведенные компьютерные эксперименты показали возможность применения разработанной модели на практике.

Ключевые слова: кибербезопасность; критерий защищенности; нечеткая логика; профиль защищенности.

A HIERARCHICAL FUZZY QUALITY ASSESSMENT OF COMPLEX SECURITY INFORMATION SYSTEMS

I. Shelechov, N. Barchenko, V. Kalchenko, V. Obodiak

Changes in the legislation of Ukraine lead to a gradual transition to international standards in the field of ensuring the protection of information in information and communication systems of government authorities. However, the latest regulatory framework is based on the regulatory documents of the past. In this regard, it became necessary to develop new approaches to assessing the security of information and communication systems. One of the options for solving this problem is the use of penetration testing methods. During this procedure, the parameters of the complex protection tools are tested using publicly available tools used by cybercriminals. After completing this procedure, three options for the results are possible, which are described by fuzzy terms: the system meets the requirements of regulatory documents, the system does not comply with the requirements of regulatory documents, the system partially meets the requirements of regulatory documents and needs to be improved. As a result, the problem arises of developing a model that allows obtaining an integral indicator of security based on a fuzzy knowledge base. The article analyzes international documents in the field of cybersecurity and normative documentation of the system of technical protection of information in Ukraine. As the criteria for evaluating the system, the criteria of security against unauthorized access were selected, which in turn are defined in the existing national regulatory documents. A model of a fuzzy hierarchical system for assessing the security profile has been developed, which sets a set of assessment criteria and the sequence of their use. The proposed hierarchical model makes it possible to present the assessment process in an explicit form and implement the process of checking the criteria, indicating the degree of confidence of the expert in the relevance of the assessment criteria. The system was implemented in the Fuzzy Logic Toolbox environment of the Matlab application package. Computer experiments have shown the possibility of applying the developed model in practice.

Keywords: cybersecurity, security criteria, fuzzy logic, security profile.

Шелехов Ігор Володимирович – канд. техн. наук, доцент, доцент кафедри комп'ютерних наук Сумського державного університету, Суми; докторант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Барченко Наталія Леонідівна – канд. техн. наук, доцент кафедри комп'ютерних наук Сумського державного університету, Суми, Україна.

Кальченко Вадим Володимирович – головний інспектор із захисту інформації Управління Держспецзв'язку в Сумській області, Суми; аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна.

Ободяк Віктор Корнелійович – канд. техн. наук, доцент, доцент кафедри комп'ютерних наук Сумського державного університету, Суми, Україна.

Igor Shelechov – PhD, Associate Professor at the Department of Computer Science, Sumy State University, Sumy; DrS-student at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: i.shelechov@cs.sumdu.edu.ua, ORCID: 0000-0003-4304-7768, Scopus Author ID: 55537177800,
https://scholar.google.com/citations?user=84_CNroAAAAJ

Nataliia Barchenko – PhD, Associate Professor at the Department of Computer Science, Sumy State University, Sumy, Ukraine,
e-mail: n.barchenko@cs.sumdu.edu.ua, ORCID: 0000-0002-5439-8750, Scopus Author ID: 55673815500, ResearcherID: W-1539-2018, https://scholar.google.com.ua/citations?user=KM_VJ-AAAAAJ&hl=ru

Vadym Kalchenko – Chief data protection officer of State service of special communication and information protection of Ukraine in Sumy region, Sumy; PhD-student at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: 0508880410@ukr.net, ORCID: 0000-0001-6492-3806.

Viktor Obodiak – PhD, Associate Professor at the Department of Computer Science, Sumy State University, Sumy, Ukraine,
e-mail: v.obodyak@cs.sumdu.edu.ua, ORCID: 0000-0002-8539-1252, Scopus Author ID: 57194526188,
https://scholar.google.com/citations?user=YXYmcSIAAAAJ&hl=ru