УДК 004.056

В.А. Лахно[1], М.М. Пойманов[2]

[1] ДНУЗТ, м. Дніпропетровськ, valss21@ukr.net

[2] ДНУЗТ, м. Дніпропетровськ, kb_dnepr@ukr.net

ВИБІР МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ДОКУМЕНТООБІГУ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

У статті запропоновано новий підхід у методології розпізнавання загроз для інформаційної безпеки (ІБ) систем документообігу (СДО) на підприємствах залізничного транспорту. запропонована інтелектуальна інформаційна технологія оцінки ступеня доцільності використання варіантів захисту СДО на основі регресійного механізму логічного висновку за рахунок використання нечітких баз знань і рівняння регресії. На основі запропонованої нечіткої регресійної моделі розроблена система підтримки прийняття рішень при діагностуванні параметрів захищеності СДО.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, РОЗПІЗНАВАННЯ, СИСТЕМИ ДОКУМЕНТООБІГУ

Вступ

Системи документообігу (СДО) є невід`ємною складовою частиною будь-якого підприємств на залізничному транспорті (ПЗТ). Від успішності функціонування цієї системи залежить керованість підприємства.

Документи СДО ПЗТ можна умовно згрупувати таким чином [1,2]:

– прогнози перевезень, виробнича програма, виробничий план, оперативні плани графіки;

– виробничі потужності, запаси;

– конструкторська документація, опис технології виробництва;

– договори на перевезення;

– фінансові документи;

– кадрова документація.

Всі документи, які функціонують на ПЗТ, можна умовно розділити на дві категорії:

– зовнішнього зв`язку,

– внутрішнього зв`язку.

До першої категорії відносяться документи, які надходять на підприємство зовні, або розробляються для передачі від підприємства іншій організації.

До другої категорії відносяться документи, за допомогою яких відбувається керування підприємством.

Серед документів як першої, так і другої категорії присутня значна кількість таких, що містять конфіденційну і навіть секретну інформацію. Тому, щоб запобігти несанкціонованому доступу (НСД) до цієї інформації, необхідно запровадити надійну систему захисту інформації (СЗІ), зокрема, документообігу. При цьому слід брати до уваги той факт, що впровадження СЗІ завжди призводить до ускладнень в роботі, отже її впровадження повинно бути економічно обґрунтованим і доцільним [1,3].

Система документообігу будь-якого підприємства містить документи на паперових носіях і електронні документи, які надходять на підприємство або створюються в результаті його функціонування. Оскільки захисту потребують всі види документів, то перейдемо до розгляду основних видів атак на системи документообігу і засобів їм протидії.

Можна виділити такі напрями захисту інформації на підприємстві:

– правові;

– організаційні;

– технічні.

1. Попередні дослідження

Розпізнавання загроз для інформаційної безпеки (ІБ) СДО ПЗТ представляє досить складний процес. Правильне визначення загроз для ІБ залежить від великої кількості різноманітних факторів, а саме: втрати інформації через збій устаткування; втрати інформації через некоректну роботу програмного забезпечення (ПЗ); втрати, пов'язані з несанкціонованим доступом; помилки обслуговуючого персоналу і користувачів, тощо. Складність розв'язання проблеми прийняття рішень багатократно зростає у випадках, коли вхідні параметри, які саме визначають стан ІБ СДО, не можуть бути виміряні точно. При цьому на практиці у більшості випадків невизначеність стану не може бути описана з використанням теоретико-ймовірнісного підходу. Це відбувається внаслідок того, що параметри не є випадковими величинами і для них не існує можливості побудувати функції розподілення. Розглянуті обставини змушують шукати нових підходів, які дозволили б вирішити завдання побудови багатовимірної залежності з нечітко заданими вхідними параметрами та нечисловою (лінгвістичною) інформацією.

Аналіз методів визначення причиново-наслідкових зв'язків між вхідними параметрами та вихідною величиною дозволяє дійти висновку, що жоден з них з притаманними їм перевагами і недоліками не може окремо повною мірою відповідати моделі "багатовимірний вхід – вихід". Отже, існує велика кількість неформалізованих задач, які не можуть бути розв'язані за допомогою лише одного методу, а необхідний консорціум методологій,

які забезпечили б основи конструювання та розвитку інтелектуальних систем розпізнавання загроз ІБ СДО ПЗТ. Першим шляхом комплексного використання таких напрямків, як нечітка логіка, нейро– і генетичні обчислення та інших інтелектуальних технологій ідентифікації стали м'які обчислення (Soft Computing), які більшою мірою пристосовані до роботи з неточними та невизначеними даними, що дозволяє розв'язати проблему лінгвістичної невизначеності [1,2,4].

Однак, наряду з подоланням труднощів використання нечітко заданої вхідної інформації необхідно також забезпечити можливість урахування відмінностей за важливістю контрольованих параметрів і врахувати їх взаємодії необхідного порядку. Ця проблема може бути вирішена методами нечіткої логіки та регресійного аналізу.

2. Постановка задачі

Таким чином, комбінація м'яких обчислень і теорії планування експерименту дає змогу формалізувати причиново-наслідкові зв'язки між змінними „вхід – вихід" та вирішити актуальну науково-практичну задачу прийняття рішень щодо розпізнавання загроз ІБ СДО за рахунок використання нечітких баз знань.

3. Результати дослідження

Зараз при проектуванні і дослідженні систем захисту інформації і систем інтелектуальної підтримки процесів підготовки і прийняття рішень стосовно інформаційної безпеки використовувалися два великі класи математичних моделей і методів: один з них представлений детермінованими, а другий імовірнісними моделями. Але в останні роки відбувається стрімкий розвиток і все більш широке застосування, абсолютно нового класу моделей і методів, заснованих на принципах теорії нечітких множин [4-6].

Перший етап моделювання нечіткими базами знань складається з формування за експертною інформацією моделі об'єкта ІБ шляхом побудови бази знань і грубого настроювання цієї моделі. Такий підхід є традиційним для нечітких систем і не гарантує збіг бажаного і модельного результату. Другий етап необхідний для проведення тонкого настроювання нечіткої моделі ІБ шляхом її навчання за експериментальними даними.

Для формалізації лінгвістичних змінних була вибрана дзвіноподібна модель функції належності, яка має найменше число параметрів, що зменшує розмірність задачі підбору цих параметрів при навчанні нечіткої моделі.

Припустимо, що проведена серія N вимірів значень контрольованих змінних показників стану системи захисту інформації (СЗІ) та інформаційної безпеки підприємства, в результаті яких отримана матриця

$$S = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1i} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2i} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{l1} & x_{l2} & \dots & x_{li} & \dots & x_{ln} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{N1} & x_{N2} & \dots & x_{Ni} & \dots & x_{Nn} \end{pmatrix}.$$

Тут вектор $X_l = (x_{l1}, x_{l2}, ..., x_{li}, ..., x_{ln})$ відповідає результатам проведення l-го експерименту із вивчення ступеню захищеності СДО підприємства. Кожному значенню x_{li} вхідної змінної x_i поставимо у відповідність m чисел $\left(z_i^{1l}, z_i^{2l}, ..., z_i^{jl}, ..., z_i^{ml}\right)$, $i = \overline{1,n}$, де z_i^{jl} – число, що встановлює, якою мірою значення x_{li} змінної x_i в l-ому експерименті сприятливо для реалізації j-го варіанту захисту СДО, $z_i^{jl} \in [0, 1]$.

Одночасно вектору X_l поставимо у відповідність m чисел $(d_{1l}, d_{2l}, ..., d_{jl}, ..., d_{ml})$, $l = \overline{1,N}$, де d_j^l – ступінь доцільності використання j-го варіанту захисту СДО за ситуації, коли набір контрольованих параметрів утворює вектор X_l, $d_j^l \in [0, 1]$.

Для j-го варіанту ІБ СДО введемо матриці

$$S_j = \begin{pmatrix} z_1^{j1} & z_2^{j1} \dots z_i^{j1} \dots z_n^{j1} & z_1^{j1} z_2^{j1} & z_1^{j1} z_3^{j1} & \dots & z_{i_1}^{j1} z_{i_2}^{j1} & \dots z_{n-1}^{j1} z_n^{j1} \\ z_1^{j2} & z_2^{j2} \dots z_i^{j2} \dots z_n^{j2} & z_1^{j2} z_2^{j2} & z_1^{j2} z_3^{j2} & \dots & z_{i_1}^{j2} z_{i_2}^{j2} & \dots z_{n-1}^{j2} z_n^{j2} \\ \dots & \dots \dots \dots \dots \dots & \dots & \dots & \dots & \dots & \dots \\ z_1^{jl} & z_2^{jl} \dots z_i^{jl} \dots z_n^{jl} & z_1^{jl} z_2^{jl} & z_1^{jl} z_3^{jl} & \dots & z_{i_1}^{jl} z_{i_2}^{jl} & \dots z_{n-1}^{jl} z_n^{jl} \\ \dots & \dots \dots \dots \dots \dots & \dots & \dots & \dots & \dots & \dots \\ z_1^{jN} & z_2^{jN} \dots z_i^{jN} \dots z_n^{jN} & z_1^{jN} z_2^{jN} & z_1^{jN} z_3^{jN} & \dots & z_{i_1}^{jN} z_{i_2}^{jN} & \dots z_{n-1}^{jN} z_n^{jN} \end{pmatrix}$$

де $D_j^T = (d_j^1 \ d_j^2 \dots d_j^l \dots d_j^N)$,

$A_j^T = (a_1{}^j \ a_2{}^j \dots a_n{}^j \ a_{12}{}^j \ a_{13}{}^j \dots a_{i1i2}{}^j \dots a_{n\text{-}1n}{}^j)$, $j = \overline{1,m}$.

Нарешті введемо модель

$$y_j^l = \sum_{i=1}^{n} a_i^j z_i^{jl} + \sum_{i_1=1}^{n} \sum_{i_2 \neq i_1} a_{i_1 i_2}^j z_{i_1}^{jl} z_{i_2}^{jl}, \qquad (1)$$

що задає ступінь доцільності використання j-го варіанту СЗІ та ІБ СДО в l-ій ситуації, $j = \overline{1,m}$.

Для розв'язання задачі оцінок ступеня доцільності D_j використання варіантів захисту СДО для будь-якого набору контрольованих параметрів при визначенні векторів-оцінок параметрів рівнянь (1) використовується методика складання і розв'язання системи нечітких логічних рівнянь. Найбільш природний підхід до розв'язання задачі розрахунку компонентів векторів $z_j = \left(z_1^j, z_2^j, ..., z_n^j\right)$ для кожного набору значень контрольованих змінних $X = (x_1, x_2, ..., x_i, ..., x_n)$ полягає в наступному. Для кожної із змінних x_i формується набір функцій належності $\psi_j(x_i)$, $j = \overline{1,m}$, $i = \overline{1,n}$, де $\psi_j(x_i)$ – функція належності контрольованої змінної x_i нечіткій множині M_{ij} значень, сприятливих для реалізації j-го варіанту захисту СДО.

Введення сукупності таких функцій належності дозволяє інтерпретувати зміряне значення кожної контрольованої змінної x_i як нечітке чис-

ло, ступінь належності якого кожній з нечітких множин M_{i1}, $M_{i2},...,M_{im}$ визначається відповідними значеннями $\psi_j(x_i)$ функцій належності.

Тоді обчислені числа $\hat{y}_1,\hat{y}_2,...,\hat{y}_j,...,\hat{y}_m$ визначають нечіткі значення ступеня доцільності використання відповідних варіантів захисту СДО для набору виміряних значень контрольованих змінних.

Розглянемо фактори, що впливають на ІБ СДО.

Застосувавши правила виконання операцій над нечіткими числами, коли функція належності контрольованого параметра x_i нечіткій безлічі значень, сприятливих для реалізації j-го варіанту, описується функцією (L-R)-типу, отримаємо функції належності нечітких чисел $\hat{y}_j$, $j=\overline{1,m}$, що визначають ступінь доцільності вибору певного рішення. Відповідне число для j-го варіанту захисту СДО ПЗТ в певній ситуації прийняття рішення при векторі контрольованих змінних $X^*=\left(x_1^*,x_2^*,...,x_n^*\right)$ дорівнює рівнянню (2).

Типи рішень щодо відповідної політики безпеки стосовно СДО вибрані наступним чином: захист СДО непотрібен (d_1); захист СДО непотрібен, потрібно оновлення системного програмного забезпечення (ПЗ) (d_2); потрібно оновлення антивірусного захисту (d_3); потрібно оновлення технічних засобів захисту інформації (ТЗЗІ) (d_4); потрібно встановлення міжмережевого екрану (МЕ) (d_5); потрібно встановлення СПВ (d_6); потрібно оновлення модулів СДО (d_7); потрібні організаційні заходи із розподілу доступу до СДО (d_8); потрібно встановлення засобів захисту від витоку інформації через інші джерела (d_9). Фактори, що впливають на вибір рішення щодо ІБ СДО, представлені у вигляді лінгвістичних змінних (табл. 1), для яких ви-

$$\psi_j\left(X^*\right)=\begin{cases} L\left(\dfrac{\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\,{x_i}^j+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\,{x_{i_1}}^j\,{x_{i_2}}^j\right)-\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\,{x_i}^*+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\,{x_{i_1}}^*\,{x_{i_2}}^*\right)}{\sum\limits_{i=1}^{n}\hat{a}_i^j\,\alpha_{ij}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\left({x_{i_1}}^j\,\alpha_{i_2j}+{x_{i_2}}^j\,\alpha_{i_1j}\right)}\right), \\ R\left(\dfrac{\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\,{x_i}^*+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\,{x_{i_1}}^*\,{x_{i_2}}^*\right)-\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\,{x_i}^j+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\,{x_{i_1}}^j\,{x_{i_2}}^j\right)}{\sum\limits_{i=1}^{n}\hat{a}_i^j\,\beta_{ij}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\left({x_{i_1}}^j\,\beta_{i_2j}+{x_{i_2}}^j\,\beta_{i_1j}\right)}\right), \end{cases} \tag{2}$$

$j=\overline{1,m}$, $\alpha>0$, $\beta>0$.

Таблиця 1

Фактори, що впливають на вибір стратегії захисту СДО, як лінгвістичні змінні

Частковий параметр стану	Універсум	Терми (T) для лінгвістичної оцінки
x_1 – рівень таємниці документів у СДО	[0,1], у. о.	некритична (нкр), критична (кр)
x_2 – режим доступу співробітників до технічних засобів СДО	[0,1], у. о.	немає (н), частковий (ч), обмежений (о)
x_3 – рівень захисту від НС копіювання	[0,1], у. о.	немає (н), незначний (нз), повний (пз)
x_4 – випадки НС знищення інформації у СДО	[0,1], у. о.	немає (н), незначні (нз), серйозні (с)
x_5 – випадки некоректної роботи ПЗ СДО	[0,1], у. о.	зафіксовані (з), незначні (нз), незафіксовані (нзф)
x_6– контроль за доступом	[0,1], у. о.	ослаблений (ос), середній (ср), нормальний (н)
x_7 – стан новизни системного ПЗ	[0,100], %	низький (н), середній (ср), нормальний (н)
x_8 – наявність криптографічних засобів у СДО	[0,100], %	низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)
x_9 – кількість інцидентів з ІБ СДО	[0,1], у. о.	немає (н), незначні (нз), часто трапляються (чт)
x_{10} – кваліфікація співробітників СДО	[0,1], у. о.	низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)
x_{11} – можливість втручання в роботу СДО ззовні	[0,100], %	низька (н), середня (с), висока (в)
x_{12} – наявність засобів резервування важливої інформації	[0,100], %	низька (н), середня (с) , висока (в)
x_{13} – втрати інформації через відмови у роботі СДО	[0,1], у. о.	легкі (л), середні (с), важкі (в)
x_{14} – наявність систем протидії вторгненням (СПВ)	[0,1], у. о.	використовуються (в), частково використовуються (чв), не використовуються (нв)
x_{15} – тип антивірусних програм	[0,1], у. о.	Безкоштовні антивіруси (б), Комерційні антивіруси (к), Комплексі системи – антивірус + фаєрвол (ка)
x_{16} – наявність процедури аудиту СДО	[0,1], у. о.	використовуються (в), частково використовуються (чв), не використовуються (нв)
x_{17} – наявність засобів ідентифікації і аутентифікації користувачів СДО	[0,1], у. о.	використовуються (в), частково використовуються (чв), не використовуються (нв)
x_{18} – наявність активних ТЗЗІ у СДО	[0,1], у. о.	мала (м), середня (с), велика (в)
x_{19} – наявність пасивних ТЗЗІ у СДО	[0,1], у. о	мала (м), середня (с), велика (в)

брані універсальні множини та терми. Тоді необхідність використовування певної стратегії захисту СДО можливо описати наступними залежностями:

$$D = f_D(x_{19}, y_4, y_5), \quad (3)$$

$$y_1 = f_1(x_3, x_4, x_5, x_6, x_7, y_3), \quad (4)$$

$$y_2 = f_2(x_9, x_{10}, x_{11}, x_{12}), \quad (5)$$

$$y_3 = f_3(x_8, x_{13}, x_{14}), \quad (6)$$

$$y_4 = f_4(x_{15}, x_{16}, x_{17}, x_{18}), \quad (7)$$

$$y_5 = f_5(x_1, x_2, y_1, y_2), \quad (8)$$

де D – стан захисту СДО, y_1, y_2, y_3, y_4, y_5 – проміжні узагальнені змінні: y_1 – стан ІБ СДО {нижче за критичний (нкр), критичний (кр), вище за критичний (вкр), високий (в)}; y_2 – вплив зовнішніх факторів {несприятливий (нс), помірний (пм), сприятливий (спв)}; y_3 – рівень забезпеченості ТЗЗІ {нижче за критичний (нкр), критичний (кр), вище за критичний (вкр), високий (в)}; y_4 – кваліфікація персоналу {низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)}; y_5 – необхідність поліпшення ІБ СДО {не потрібно, оновлення системного ПЗ (опз), оновлення антивірусного захисту (оаз), встановлення СПВ (спв)}.

Для кожного із співвідношень (3)-(8) будуються нечіткі бази знань, які представляють сукупність нечітких правил «ЯКЩО-ТОДІ», що визначають взаємозв'язок між вхідними та вихідною змінними. За нечіткими базами знань складаються логічні рівняння. Скорочена система логічних рівнянь, що відповідає співвідношенню (3), виглядає наступним чином:

$$\psi^{d_j}(D) = \bigvee_{p=1}^{h_j} \left[\psi^{y_4^{jp}}(y_4) \wedge \psi^{y_5^{jp}}(y_5) \wedge \psi^{x_{19}^{jp}}(x_{19}) \right], \quad (9)$$

$$p = \overline{1, h_j}, \; j = \overline{1, 9}$$

де $\psi^{y_4^{jp}}(y_4)$, $\psi^{y_5^{jp}}(y_5)$, $\psi^{x_{19}^{jp}}(x_{19})$ – функції належності змінних y_4, y_5, x_{19} до їх нечітких термів y_4^{jp}, y_5^{jp}, x_{19}^{jp} відповідно; $\vee$ – логічне АБО, $\wedge$ – логічне І, як операції *max* і *min* відповідно.

На рис. 1 представлені результати дослідження. Як видно із діаграми більшість параметрів стану x_i^* для організації в якій виконувалось дослідження знаходиться в допустимих межах, див. табл. 2. Як показали результати дослідження найбільшої уваги потребують такі параметри, як наявність криптографічних засобів у СДО та необхідність додаткового резервування інформаційних та програмних масивів через загрозу втрати інформації, пов'язані із через потенційними відмовами у роботі СДО. Оцінки ступеня доцільності прийняття рішення щодо визначення захищеності СДО виконувалася на основі обробки даних анкетування фахівців ПЗД (м. Дніпропетровськ) з використанням розробленого регресійного механізму логічного висновку.

Таблиця 2

Рівні захисту СДО

Рівень	Значення
1	Низький рівень захисту
2	Недостатній захист
3	Достатній захист
4	Хороший захист
5	Дуже добрий захист

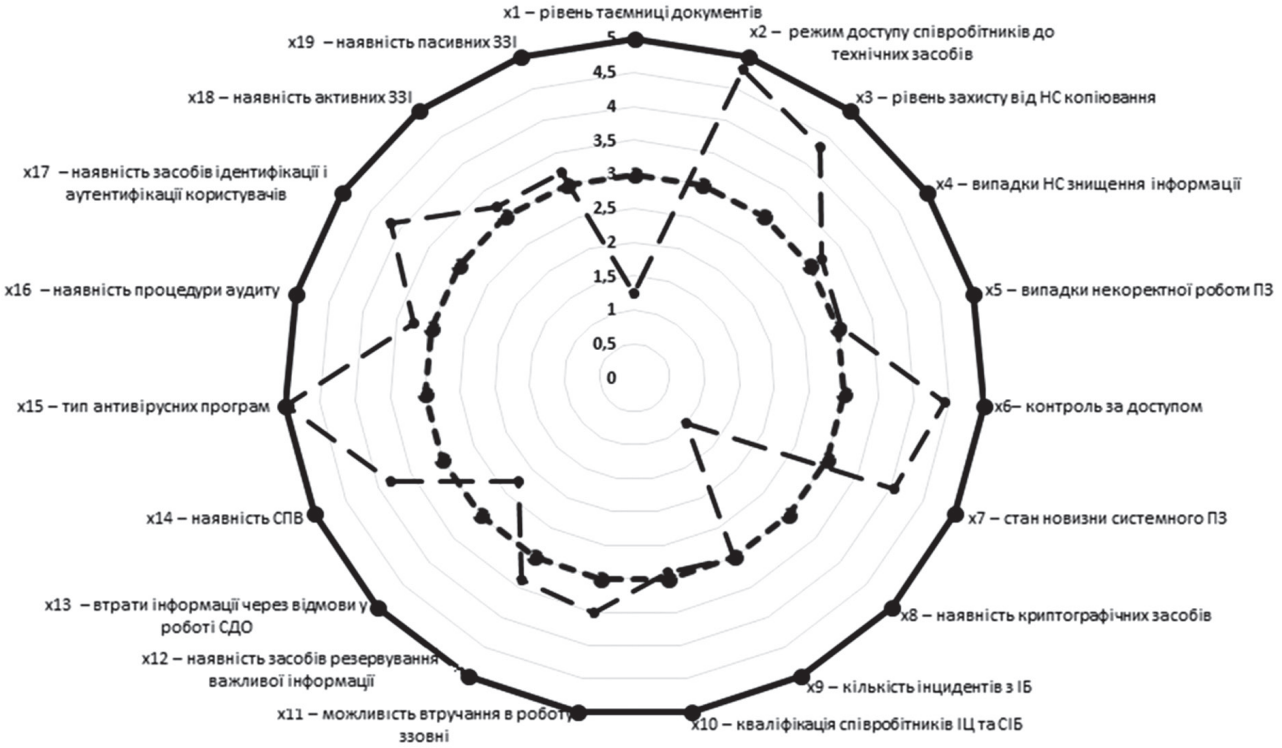

Рис. 1. Результати дослідження лінгвістичних змінних, що впливають на вибір стратегії захисту СДО

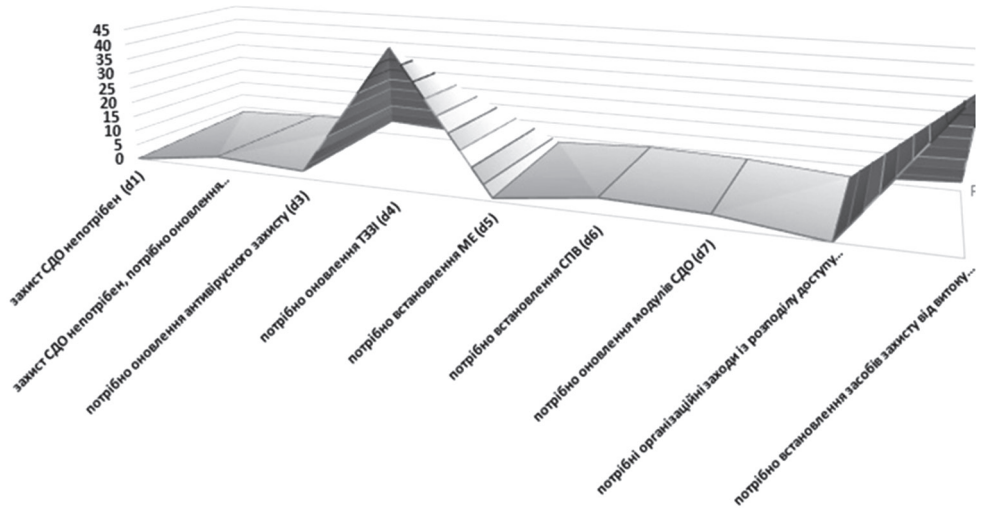

Рис. 2. Результати дослідження типів рішень щодо політики ІБ СДО

Висновки

Таким чином, в роботі запропонована методика та інтелектуальна інформаційна технологія оцінки ступеня доцільності використання варіантів захисту СДО на основі регресійного механізму логічного висновку за рахунок використання нечітких баз знань і рівняння регресії.

Запропонована методика дозволяє для будь-якого набору контрольованих параметрів розраховувати ступінь доцільності використання кожного з 9 можливих варіантів підвищення ступеню захищеності СДО та обрати той з них, ступінь доцільності якого є найбільшою.

Список літератури: 1. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных / Герасименко В.А. В 2-х кн. – М.: Энергоатомиздат, 1994. Т1. С. 132-138. **2.** *Лахно В.А.* Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок. Монография. / В.А. Лахно, А.С Петров. – Луганск: изд-во ВНУ им. В. Даля, 2010. – 280 с. **3.** *Борисов А.Н.* Принятие решения на основе нечетких моделей: примеры использования / А. Н. Борисов, О. А. Крумберг, И. П. Федоров. – Рига: Знание, 1990. – 184 с. **4.** *Новіков О.* Побудова логіко-ймовірностної моделі захищеної комп'ютерної системи / О. Новіков, А. Тимошенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 3. – с. 101 – 105. **5.** *Риндюк В. О.* Організація систем захисту інформації на основі методів нечітких множин: дисертація канд. техн. наук: 05.13.21 / НАН України; Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова. – К., 2003. **6.** V. Lahno. Ensuring security of automated information systems, transportation companies with the intensification of traffic / V. Lahno, A. Petrov.: Monograph. Lugansk. 2011. – 190 p.

Надійшла до редколегії 10.03.2015

УДК 004.056

Выбор методов защиты информации в системах документооборота железнодорожного транспорта / В. А. Лахно, М. Н. Пойманов // Бионика интеллекта: научн.-техн. журнал. – 2015. – № 1 (84). – С. 91–95.

В статье предложен новый подход в методологии распознавания угроз для информационной безопасности (ИБ) систем документооборота (СДО) на предприятиях железнодорожного транспорта. На основе предложенной нечеткой регрессионной модели разработана система поддержки принятия решений при диагностировании параметров защищенности СДО, которая работает под управлением операционной системы Windows и не требует специальной подготовки.

Табл. 2. Ил. 2. Библиогр.: 6 назв.

UDK 004.056

The choice of methods of information security in document management systems of railway transport / V. A. Lahno, M. N. Poimanov // Bionics of Intelligense: Sci. Mag. – 2015. – №1 (84). – P. 91–95.

This paper proposes a new approach to recognition methodology threats to information security (IS) document management systems (DMS) on railway transport enterprises. Based on the proposed fuzzy regression model developed a decision support system for diagnosing security settings DMS. Decision support system running the Windows operating system and requires no special training.

Tab. 2. Fig. 2. Ref.: 6 items.