УДК 004.056.53:656.078

ІНФОРМАЦІЙНА БЕЗПЕКА ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ

Валерій Лахно

Стаття містить результати досліджень, присвячених подальшому розвитку моделей розпізнаванні загроз інформаційно-комунікаційному середовищу інтелектуальних транспортних систем на наземному транспорті та удосконаленню інформаційної безпеки в умовах впровадження нових та модернізації існуючих інформаційних систем, і збільшення кількості дестабілізуючих впливів на доступність, конфіденційність і цілісність інформації. Запропонований новий підхід прийняття рішень для забезпечення інформаційної безпеки інтелектуальних систем наземного транспорту при певному векторі вхідних параметрів на основі нечіткого регресійного механізму логічного висновку для системи підтримки прийняття рішень з нечіткими початковими даними.

Ключові слова: *інтелектуальні транспортні системи, захист інформації, інформаційна безпека, розпізнавання загроз, нечіткі множини.*

Вступ. В даний час одним з найбільш перспективних напрямків розвитку транспортних технологій в розвинених країнах світу є розробка та впровадження інтелектуальних транспортних систем (ІТС). ІТС дозволяють більш ефективно реалізовувати низку глобальних технологій перевезення вантажів і пасажирів [1-4]. Наочними прикладами інтелектуальних транспортних технологій (ІТТ) є «інтелектуальний вантаж», який може автоматично повідомляти власнику про свої властивості, технології «відстеження вантажів», забезпечення автоматичного управління рухомими об'єктами та інші [2, 3, 5-7]. ІТТ містять ряд характерних компонентів, що виконують автоматичний збір даних про умови перевезень, моделювання процесів, порівняння даних із встановленими нормативами, розпізнавання нештатних ситуацій, прогнозування станів ІТС, планування перевезень та ін., див. рис.1.

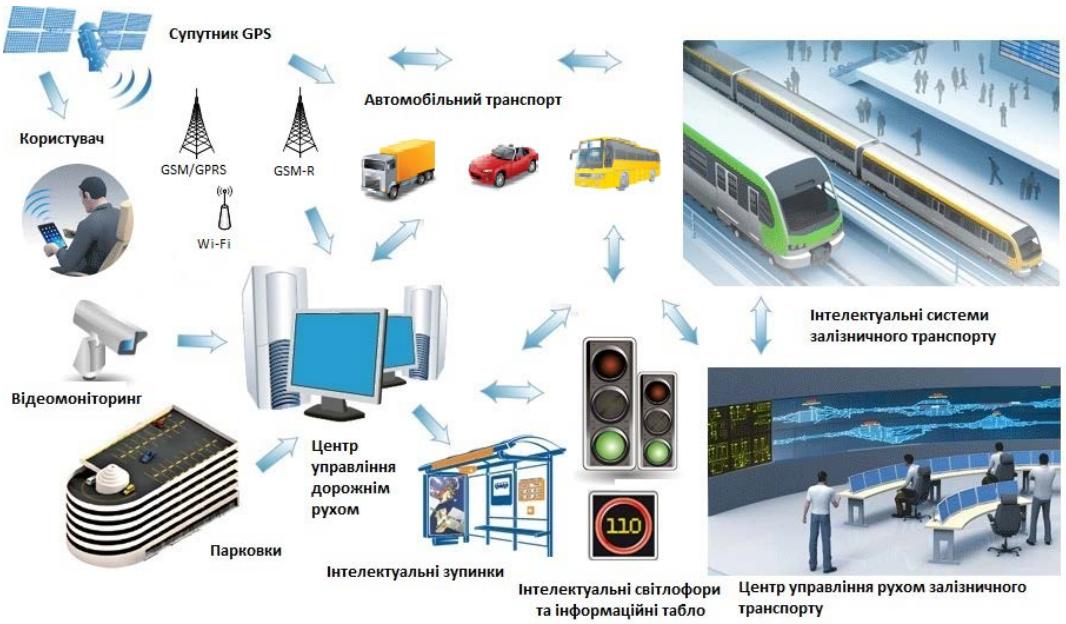

Рис. 1. ІТС наземного транспорту

Аналіз існуючих досліджень. Активне розширення інформаційно-комунікаційних систем транспорту (ІКСТ), у тому числі у ІТС, супроводжується виникненням нових загроз для інформаційної безпеки (ІБ), про що свідчить зростання числа інцидентів пов'язаних із захистом інформації [8-12], а також виявлених уразливостей у інформаційних системах (ІС) та автоматизованих системах управління (АСУ) на транспорті [13, 14, 15].

Об'єктом атаки (комп'ютерного нападу на інформацію – КНІ) може стати будь-який з елементів ІКСТ. Проте в цілому всі елементи ІКСТ можуть бути віднесені до однієї з трьох категорій: центри обробки даних (ЦОД), АСК, АІС, ІС; пе-

риферійне обладнання та PLC; системи та канали зв'язку для обміну даними [12, 14, 15, 16, 17, 19].

У зловмисників є кілька точок входу, щоб скомпрометувати ІТС. ІКСТ та ІТС можуть бути заражені різними способами, наприклад, вірус (експлойт) може бути впроваджений через USB-з'єднання або через мережевий інтерфейс.

Як правило, кількість виявлених уразливостей корелює з кількістю опублікованих експлойтів, наприклад з лютого 2011 р. по вересень 2013 р. було опубліковано 150 експлойтів [12, 13, 18], тобто, це в вісім разів більше, ніж за період з 2005 р. по 2010 р.

Не варто скидати з рахунків і DDoS/DoS атаки на ІТС, в результаті яких знижується рівень ІБ. Реальний приклад використовування зловмисниками КНІ - DDoS/DoS у транспортних SCADA системах зафіксовано у 2012 р. коли зловмисники блокували протягом години роботу метрополітену у Чанчжэні (КНР) [13].

Уразливість ІТС обумовлена відсутністю механізмів безпеки в промислових протоколах і системах відповідно до проекту, уразливістю ПЗ та його некоректною конфігурацією. Необхідність інтеграції з зовнішніми мережами (корпоративними, WAN, Інтернет), використання бездротових мереж і відкритих інформаційних технологій - ОС, мережевих протоколів і служб, віддаленого доступу - теж не сприяють безпеці АСК ТГ.

Отже, актуальність досліджень, спрямованих на подальший розвиток моделей та методів захисту на основі інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту та забезпечення ІБ ІТС в постійного зростання кількості дестабілізуючих впливів, є однією з ключових проблем захисту інформації об'єктів транспортної інфраструктури держави.

Метою даної роботи є апробація нових моделей розпізнавання загроз для ІБ ІКСТ, які, на відміну від існуючих, дозволяють прийняти остаточне рішення про наявність або відсутність загрози в межах існуючих та нових класів вторгнень у ІТС.

Основна частина дослідження. В силу того, що системи розпізнавання загроз для ІТС ще підлягають своєї реалізації, формалізована постановка задачі для їх розробки може бути сформульована таким чином.

Вихідними даними для всіх ІС є дані, що містяться в репозиторії REP:

$$REP = \langle SYS, Events, TAI, NIS, gov \rangle, \quad (1)$$

де SYS - дані про інфраструктуру ІТС яка підлягає захисту (топологія, склад елементів, користувачі та ін.); $Events$ - дані про події ІБ, які пройшли попередню обробку і знаходяться в репозиторії на зберіганні; TAI - дані про сценарії атак (нападів на інформацію) у вигляді шаблонів; NIS - дані про інциденти з ІБ, можливі контрзаходи і т. п.; gov - вирішальне (розв'язувальне) в рамках політики безпеки (ПБ) [12].

Наприклад, дані про дані про сценарії атак описуються у вигляді наступних кортежем:

$$TAI^{ea} = \langle MI, PA, S^{\text{ea}}, CE, DP, P, AO(NS) \rangle, \quad (2)$$

$$TAI^{ia} = \langle MI, PA, S^{\text{ia}}, CE, DP, P, AO^{k}(NS_{m}^{k}) \rangle, \quad (3)$$

де TAI^{z} – віддалена атака на ІТС, наприклад, використовуючи мережу Wi-Fi; TAI^{ia} – внутрішня атака на компоненти ІТС рівня критичності k; MI - загальне число загроз для ІБ ІТС; PA - число можливих цілей порушника в ІТС; S^{ea} – джерела зовнішніх загроз; S^{ia} – джерела внутрішніх загроз; CE – комунікаційне обладнання ІТС; DP - засоби захисту інформації (ЗЗІ) та забезпечення ІБ на шляху поширення атаки; P – протоколи, пакети у ІТС; AO – об'єкт доступу у ІТС; NS_m^k – сегмент, в якому опрацьовується інформація, найвищий рівень критичності якої дорівнює k; m – номер сегменту ІКС ІТС.

Завдання, які вирішуються ЗЗІ можуть бути записані таким чином:

$$IOFP_j = FS(SYS, TAI, AT, gov), \quad (4)$$

де $IOFP_j$ - значення j - го показника захищеності ІТС; AT - події ІБ, що відображають атаку на ІТС; FS - функція яка визначає $IOFP_j$ на основі прийнятої ПБ.

Управління кореляцією ПБ для ІТС:

$$K_{\text{event}} = F\text{Cor}\{\text{e}_\text{i}\}, \quad (5)$$

де K_{event} - критична подія ІБ; $e_i \subset Events$; FCor - функція кореляції, яка дозволяє на основі аналізу подій з ІБ (зберігаються в репозиторії REP), виявляти критичні події.

Моделювання атак на ІТС:

$$ESC_{cr} = Model(SYS, TAI, AT, gov, T), \quad (6)$$

де $ESC_{cr} \subset SYS$ - критичний елемент ІТС; $Model$ - модель атаки у часі - T.

Підтримка прийняття рішень (або експертна система):

$$CM = \arg \min \left| IOFP - IOFP_{\text{requirement}} \right|, \quad (7)$$

де $CM \subset gov$ - оптимальний контрзахід (ЗЗІ), що є елементом вирішального правила в рамках ПБ для ІТС; $IOFP$ та $IOFP_{\text{requirement}}$ - поточне та еталонне значення показника захищеності, відповідно.

Найбільш складним, на наш погляд, є етап розпізнавання загроз для ІБ ІТС. Правильне визначення загроз для ІБ залежить від великої кіль-

кості різноманітних факторів, а саме: втрати інформації через збій устаткування ІКС та ІТС, в цілому; втрати інформації через некоректну роботу програмного забезпечення (ПЗ) ІТС; втрати, пов'язані з несанкціонованим доступом (НСД); помилки обслуговуючого персоналу і користувачів, тощо. Складність розв'язання проблеми прийняття рішень багатократно зростає у випадках, коли вхідні параметри, які саме визначають стан ІБ ІТС, не можуть бути виміряні точно. Це, у свою чергу, змушує розробників систем захисту інформації (СЗІ) шукати нових підходів, які дозволили б вирішити завдання побудови багатовимірної залежності з нечітко заданими вхідними параметрами та нечисловою (лінгвістичною) інформацією [20-22].

Перший етап моделювання нечіткими базами знань складається з формування за експертною інформацією моделі ІБ ІТС 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 [20, 21].

Припустимо, що проведена серія N вимірів значень контрольованих змінних показників стану ІБ ІТС, 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 $X_l = (x_{l1}, x_{l2},\dots,x_{li},\dots,x_{ln})$ відповідає результатам проведення l-го експерименту із вивчення ступеню захищеності ІТС. 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 ІТС, $z_i^{jl} \in [0, 1]$.

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

Для j-го варіанту ІБ ІТС введемо матриці

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

де $D_j^T = (d_j^1\ \ d_j^2\ \dots\ d_j^l\ \dots\ d_j^N)$, $A_j^T = (a_1^j\ \ a_2^j\ \dots\ a_n^j\ \ a_{12}^j\ \ a_{13}^j\ \dots\ a_{i1i2}^j\ \dots\ a_{n-1n}^j)$, $j=\overline{1,m}$.

Введемо модель що задає ступінь доцільності використання j-го варіанту системи захисту інформації (СЗІ) та ІБ ІТС в l-ій ситуації, $j=\overline{1,m}$

$$y_j^l = \sum_{i=1}^{n} a_i^j z_i^{jl} + \sum_{i_1=1}^{n}\sum_{i_2\neq i_1} a_{i_1i_2}^j z_{i_1}^{jl} z_{i_2}^{jl}\ . \qquad (8)$$

Для розв'язання задачі оцінок ступеня доцільності D_j використання варіантів захисту ІТС для будь-якого набору контрольованих параметрів при визначенні векторів-оцінок параметрів рівнянь (8) 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 $X = (x_1, x_2,\dots,x_i,\dots,x_n)$ 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 ІТС.

Введення сукупності таких функцій належності дозволяє інтерпретувати зміряне значення кожної контрольованої змінної x_i як нечітке число, ступінь належності якого кожній з нечітких множин $M_{i1}, M_{i2},\dots,M_{im}$ 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 вико-

ристання відповідних варіантів СЗІ ІТС для набору виміряних значень контрольованих змінних.

Розглянемо фактори, що впливають на ІБ ІТС. 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 ІТС в певній ситуації прийняття рішення при векторі контрольованих змінних $X^*=\left(x_1^*, x_2^*, \ldots, x_n^*\right)$ дорівнює рівнянню (9). Типи рішень щодо відповідної ПБ стосовно ІТС вибрані наступним чином: захист ІТС непотрібен (d_1); захист ІТС непотрібен, потрібно оновлення системного 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 системи протидії вторгненням (СПВ) (d_6); потрібно оновлення ПЗ модулів ІТС (d_7); потрібні організаційні заходи із розподілу доступу до компонентів ІТС (d_8); потрібно встановлення засобів захисту від витоку інформації через інші джерела (d_9).

$$\psi_j\left(X^*\right)=\begin{cases} L\left(\dfrac{\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\, xi^{\,j}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\, xi_1^{\,j}\, xi_2^{\,j}\right)-\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\, xi^{\,*}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\, xi_1^{\,*}\, xi_2^{\,*}\right)}{\sum\limits_{i=1}^{n}\hat{a}_i^j\,\alpha_{ij}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\left(xi_1^{\,j}\,\alpha_{i_2j}+xi_2^{\,j}\,\alpha_{i_1j}\right)}\right), \\ R\left(\dfrac{\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\, xi^{\,*}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\, xi_1^{\,*}\, xi_2^{\,*}\right)-\left(\sum\limits_{i=1}^{n}\hat{a}_i^j\, xi^{\,j}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\, xi_1^{\,j}\, xi_2^{\,j}\right)}{\sum\limits_{i=1}^{n}\hat{a}_i^j\,\beta_{ij}+\sum\limits_{i_1=1}^{n}\sum\limits_{i_2\neq i_1}\hat{a}_{i_1i_2}^j\left(xi_1^{\,j}\,\beta_{i_2j}+xi_2^{\,j}\,\beta_{i_1j}\right)}\right), \end{cases} \quad (9)$$

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

Фактори, що впливають на вибір рішення щодо СЗІ ІТС, представлені у вигляді лінгвістичних змінних (табл. 1), для яких вибрані універсальні множини та терми. Тоді необхідність використовування певної стратегії захисту ІТС можливо описати так:

$$D=f_D(x_{19},y_4,y_5), \quad (10)$$
$$y_1=f_1(x_3,x_4,x_5,x_6,x_7,y_3), \quad (11)$$
$$y_2=f_2(x_9,x_{10},x_{11},x_{12}), \quad (12)$$
$$y_3=f_3(x_8,x_{13},x_{14}), \quad (13)$$
$$y_4=f_4(x_{15},x_{16},x_{17},x_{18}), \quad (14)$$
$$y_5=f_5(x_1,x_2,y_1,y_2), \quad (15)$$

де D – стан захисту ІТС, y_1, y_2, y_3, y_4, y_5 – проміжні узагальнені змінні: y_1 – стан ІБ ІТС {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 {(нкр), (кр), (вкр), (в)}; y_4 – кваліфікація персоналу {низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)}; y_5 – необхідність поліпшення ІБ ІТС {не потрібно, оновлення системного ПЗ (опз), оновлення антивірусного захисту (оаз), встановлення СПВ (спв)} Для кожного із співвідношень (10)-(15) 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 виглядає наступним чином:

$$\psi^{d_j}(D)=\bigvee_{p=1}^{h_j}\left[\psi^{y_4^{jp}}(y_4)\wedge\psi^{y_5^{jp}}(y_5)\wedge\psi^{x_{19}^{jp}}(x_{19})\right] \quad (16)$$

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

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.

Таблиця 1

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

Частковий параметр стану	*Універсум*	*Терми (Т) для лінгвістичної оцінки*
x_1 – рівень таємниці інформаційних ресурсів ІКС та ІТС	[0,1], у. о.	некритична (нкр), критична (кр)
x_2 – режим доступу співробітників до компонентів ІКС та ІТС	[0,1], у. о.	немає (н), частковий (ч), обмежений (о)
x_3 – рівень захисту від НСД до ІКС та ІТС	[0,1], у. о.	немає (н), незначний (нз), повний (пз)
x_4 – випадки НСД до ІКС та ІСТ	[0,1], у. о.	немає (н), незначні (нз), серйозні (с)
x_5 – випадки некоректної роботи ПЗ	[0,1], у. о.	зафіксовані (з), незначні (нз), незафіксовані (нзф)
x_6 – контроль за доступом до ІТС	[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	[0,100], %	низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)
x_9 – кількість інцидентів з ІБ у ІТС	[0,1], у. о.	немає (н), незначні (нз), часто трапляються (чт)
x_{10} – кваліфікація співробітників	[0,1], у. о.	низька (н), нижче за середню (нс), середня (с), вище за середню (вс), висока (в)
x_{11} – можливість втручання в роботу ІТС ззовні	[0,100], %	низька (н), середня (с), висока (в)
x_{12} – наявність засобів резервування	[0,100], %	низька (н), середня (с) , висока (в)
x_{13} – втрати інформації через відмови у роботі ПЗ	[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 ІБ ІТС	[0,1], у. о.	використовуються (в), частково використовуються (чв), не використовуються (нв)
x_{17} – наявність засобів ідентифікації і аутентифікації користувачів	[0,1], у. о.	використовуються (в), частково використовуються (чв), не використовуються (нв)
x_{18} – наявність активних ТЗЗІ у ІТС	[0,1], у. о.	мала (м), середня (с), велика (в)
x_{19} – наявність пасивних ТЗЗІ у ІТС	[0,1], у. о	мала (м), середня (с), велика (в)

Результати дослідження. Для вирішення деяких питань у ході досліджень була розроблена експертна система (ЕС) «Аналізатор загроз» [12], зокрема, призначена для розпізнавання загроз ІБ та збору інформації про стан комп'ютерного обладнання у мережі ІТС. В основу роботи ЕС покладено припущення про те, що елементи множини функцій безпеки можуть не повністю забезпечувати виконання вимог ІБ на підприємстві, а отже, призводити до зростання показника поточних інформаційного ризиків [12]. Задається рівень поточного інформаційного ризику, який вважається прийнятним і не вимагає вживання дорогих заходів протидії спробам НСД.

Програма включає в себе кілька модулів, що можуть функціонувати і як єдиний комплекс, і у вигляді самостійних програмних продуктів, див. рис. 2.

На рис. 3 представлені результати дослідження стану ІБ елементів ІТС. Як видно із діаграми більшість параметрів стану x_i^* для організації в якій виконувалось дослідження знаходиться в допустимих межах.

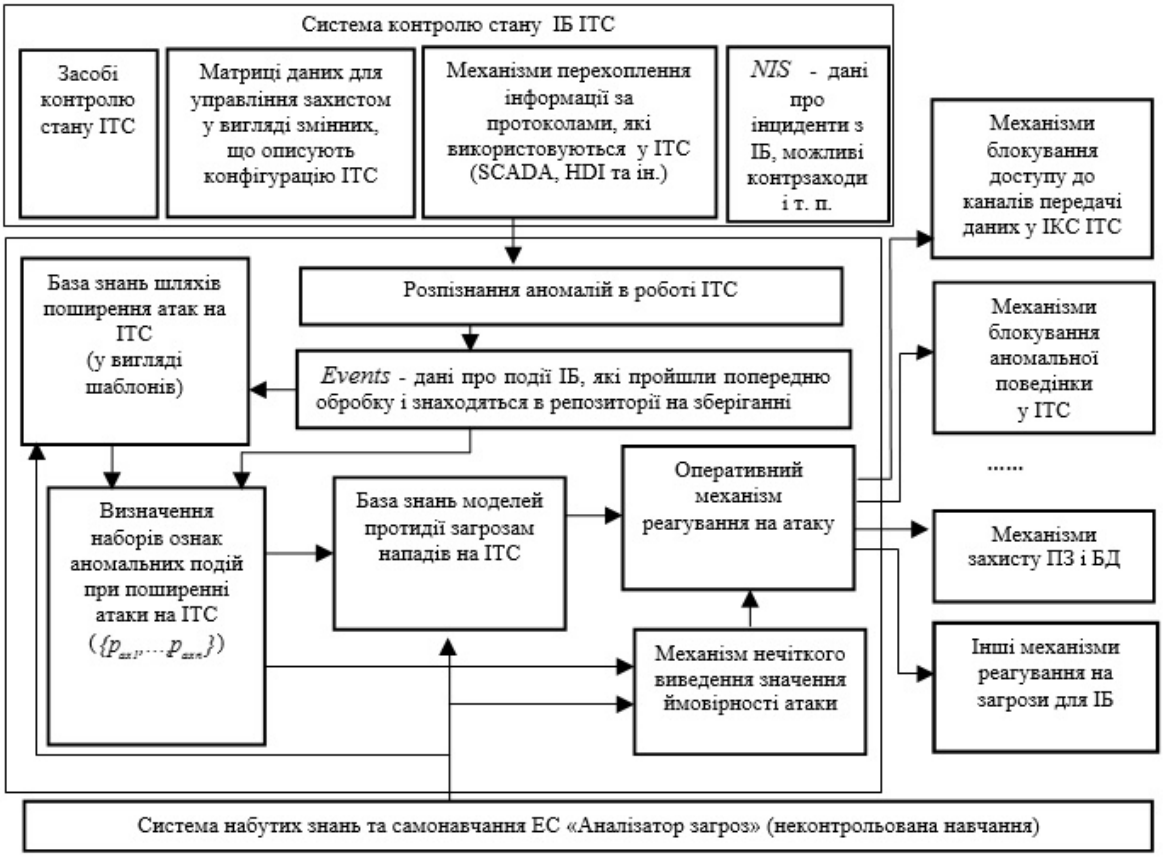

Рис. 2. Структура модулів ЕС «Аналізатор загроз»

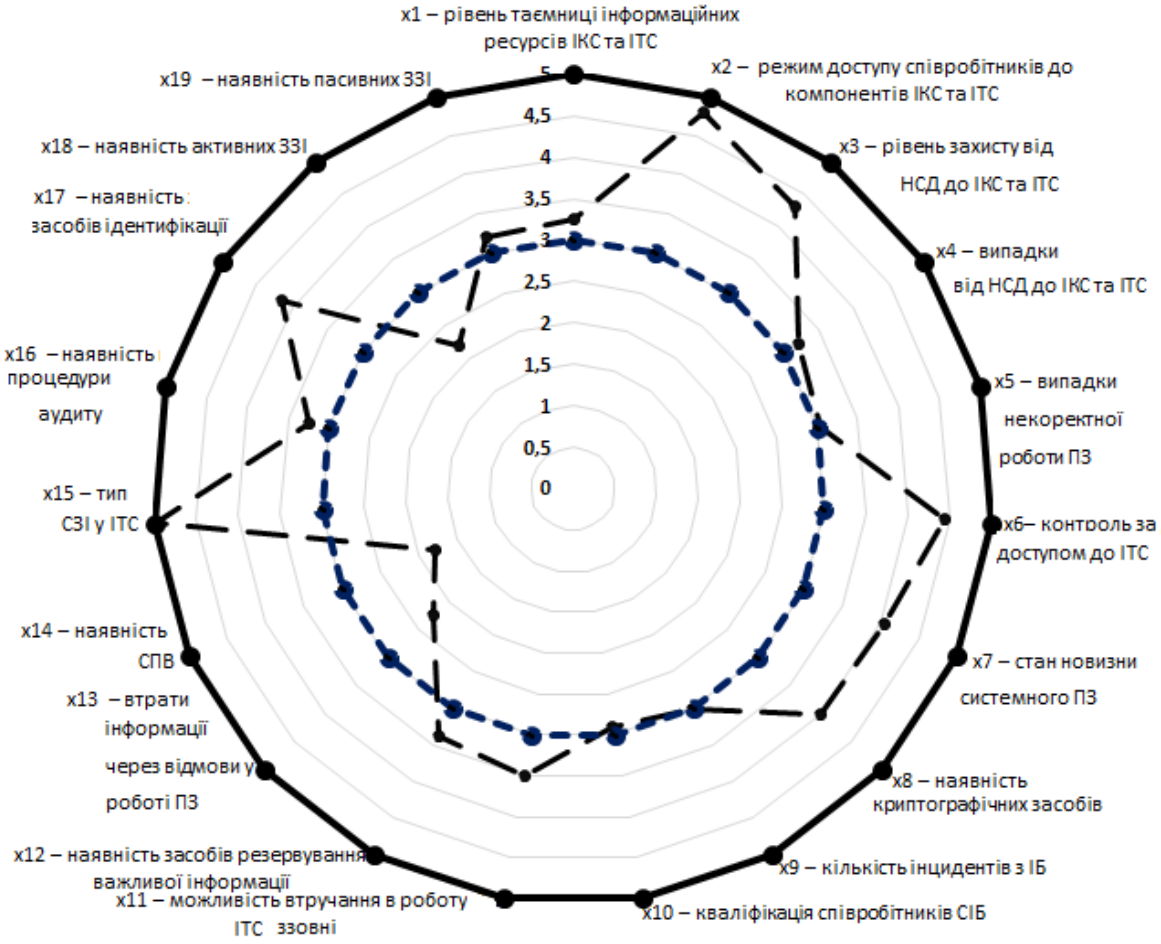

Рис. 3. Результати дослідження стану ІБ елементів ІТС

Висновки

Як показали результати дослідження найбільшої уваги потребують такі параметри, як наявність систем протидії вторгненням у ІТС та необхідність додаткових засобів пасивного захисту інформації яка опрацьовується у ІТС. Оцінки ступеня доцільності прийняття рішення щодо визначення захищеності ІТС виконувалася на основі обробки даних анкетування фахівців (м. Київ, Харків, Дніпропетровськ) з використанням розробленого регресійного механізму логічного висновку.

При вирішенні завдань інтелектуального розпізнавання загроз для ІБ ІТС з використанням представницьких наборів довелося відмовитися від вимоги безвихідності представницького набору, тому що перевірка безвихідності значно знижує швидкість роботи алгоритму.

ЛІТЕРАТУРА

[1]. The role of IT in logistics / David J. Closs, Jim Davidson, Richard L. Dawe, Templeton S. J., Levitt K. A. // The Official Magazine of the Logistics Institute, 2007, Vol. 27. № 6.

[2]. Transport Logistics. Shared solution to common challenges/ ODSE, 2002. - 53 p.

[3]. Transportation & Logistics 2030. Volume 4: Securing the supply. – pp. 254-286.

[4]. Интеллектуальные транспортные системы железнодорожного транспорта (основы инновационных технологий) [Текст]: пособие / В.В. Скалозуб, В.П. Соловьев, И.В. Жуковицкий, К.В. Гончаров. – Д.: Изд-во Днепропетр. нац. ун-та ж.-д. трансп. им. акад. В. Лазаряна, 2013. – 207 с.

[5]. Автоматизированные системы обработки информации и управления на автомобильном транспорте [Текст] / А.Б. Николаев, С.В. Алексахин, И.А. Кузнецов, В.Ю. Строганов [и др.]; Под ред. А.Б. Николаева. - М.: Издательский центр «Академия», 2003. – 224 с.

[6]. Intelligent Transport Systems (ITS) for sustainable mobility. UN, Economic Commission for Europe, UNECE. Geneva, February 2012. – 120 pp.

[7]. Modern Transport Telematics / Ed. Jerzy Mikulski //11th International Conference on Transport Systems Tlematics, TST 2011. Katowice-Ustron, Poland, October 19-22, 2011. – 418 p.

[8]. Корниенко А.А. Средства защиты информации на железнодорожном транспорте. [учеб. пос.] / А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров. - М.: Маршрут, 2006. – 256 с.

[9]. John R. Vacca. Managing Information Security. Syngress – 2010. – 320 pp.

[10]. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin. Firewalls and Internet Security, 2nd Edition. Addison Wesley – 2003. – 464 pp.

[11]. Bragg R., Rhodes-Ousley M, Keith E. Network Security. Strassberg Osborne/McGraw-Hill – 2003. – 896 pp.

[12]. 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.

[13]. MITRE Research Program. [Электронный ресурс]: Режим доступу: http://www.mitre.org

[14]. The Web Hacking Incidents Database 2008: Annual Report. [Электронный ресурс]: Режим доступу: http://www.breach.com/confirmation/2008 WHID.html

[15]. Mirkovic J. Internet Denial of Service: Attack and Defense Mechanisms. / Mirkovic J., Dietrich S., Dittrich D., Reiher P. – Prentice Hall PTR, 2004. 400 p.

[16]. Unsupervised adaptive filtering. V. 1, 2. Edited by S. Haykin. – New York: John Willey & Sons, Inc, 2000. – 1206 p.

[17]. Uptime Protection Solution. Nexusguard. Survey of Network – Based Defense Mechanisms Countering the DoS and DDoS Problems. April 2014.

[18]. Давиденко А.М. Аналіз дій загроз у автоматизованих системах обробки інформації / Давиденко А.М., Головань С.М., Щербак Л.М. // Моделювання та інформаційні технології Зб. наук. Пр. ІПМЕ НАН України. – 2006. – Вип. № 36. – С. 3-8.

[19]. Домарев В.В. Безопасность информационных технологий. Системный подход [Текст] / Домарев В.В. – К.: ТОВ «ТВД ДС», 2004. – 992 с.

[20]. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения [Текст] / Корченко А.Г. – К.: «МК-Пресс», 2006. – 320 с.

[21]. Kaufmann, A. and Gupta, M.M. Introduction to fuzzy arithmetic: Theory and Applications, Van Nostrand Reinhold, New York, 1991, – 361 p.

[22]. Zimmermann H.-J. Fuzzy Set Theory – and Its Applications, Kluwer Academic Publishers, Boston/Dordrecht/London, 1992, – 399 p.

REFERENCES

[1]. The role of IT in logistics / David J. Closs, Jim Davidson, Richard L. Dawe, Templeton S. J., Levitt K. A. // The Official Magazine of the Logistics Institute, 2007, Vol. 27. № 6.

[2]. Transport Logistics. Shared solution to common challenges/ ODSE, 2002, 53 p.

[3]. Transportation & Logistics 2030. Volume 4: Securing the supply., pp. 254-286.

[4]. V.V. Skalozub, V.P. Solovev, I.V. Zhukovitskiy, K.V. Goncharov. Intellectual transport systems of railway transport (based on innovative technologies). Textbook. Dnipropetrovsk: DNURT, 2013, 207 p.

[5]. Automated systems for information processing and management of road transport. Textbook. Ed. A.B. Nikolaev. M.: Academy, 2003, 224 p.

[6]. Intelligent Transport Systems (ITS) for sustainable mobility. UN, Economic Commission for Europe, UNECE. Geneva, February 2012, 120 p.
[7]. Modern Transport Telematics / Ed. Jerzy Mikulski //11th International Conference on Transport Systems Tlematics, TST 2011. Katowice-Ustron, Poland, October 19-22, 2011, 418 p.
[8]. A.A. Kornienko, M.A. Eremeev, S.E. Adadurov. The means of information security on railway transport. Textbook. M.: Marshrut, 2006, 256 p.
[9]. John R. Vacca. Managing Information Security. Syngress. 2010, 320 p.
[10]. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin. Firewalls and Internet Security, 2nd Edition. Addison Wesley, 2003, 464 p.
[11]. Bragg R., Rhodes-Ousley M, Keith E. Network Security. Strassberg Osborne/McGraw-Hill. 2003, 896 p.
[12]. V.A. Lahno, A.S. Petrov. Ensuring the security of automated information systems of transport enterprises at an intensification of traffic. Monograph, Lugansk.: VNU, 2010, 280 p.
[13]. MITRE Research Program. / http://www.mitre.org
[14]. The Web Hacking Incidents Database 2008: Annual Report. / http://www.breach.com /confirmation/2008 WHID.html
[15]. Mirkovic J. Internet Denial of Service: Attack and Defense Mechanisms. / Mirkovic J., Dietrich S., Dittrich D., Reiher P. – Prentice Hall PTR, 2004, 400 p.
[16]. Unsupervised adaptive filtering. V. 1, 2. Edited by S. Haykin. – New York: John Willey & Sons, Inc, 2000, 1206 p.
[17]. Uptime Protection Solution. Nexusguard. Survey of Network – Based Defense Mechanisms Countering the DoS and DDoS Problems. April 2014.
[18]. Davidenko A.M., Golovan S.M., Scherbak L.M. The analysis of actions of threats in automated information processing systems // Modelling and Information Technology. Vol. 36. 2006, pp. 3-8.
[19]. Domarev V.V. Safety of information technology. System method. K.: TOV «TVD DS», 2004, 992 p.
[20]. Korchenko A.G. Creation of systems of information security on indistinct sets. Theory and practical decisions. K.: « MK-Press », 2006, 320 p.
[21]. Kaufmann, A. and Gupta, M.M. Introduction to fuzzy arithmetic: Theory and Applications, Van Nostrand Reinhold, New York, 1991, 361 p.
[22]. Zimmermann H.-J. Fuzzy Set Theory – and Its Applications, Kluwer Academic Publishers, Boston/Dordrecht/London, 1992, 399 p.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Для повышения информационной безопасности интеллектуальных транспортных систем необходимо проводить исследования, направленные на дальнейшее развитие методов и моделей распознавании угроз информационно-коммуникационной среде транспорта и принятия решений при нечетко заданной входной информации. Предложен новый подход для принятия решений, направленных на обеспечение информационной безопасности интеллектуальных систем наземного транспорта при заданном векторе входных параметров на основе нечеткого регрессионного механизма логического вывода для системы поддержки принятия решений с нечеткими исходными данными. Предложена диагностическая модель обеспечивающая более точное определение параметров информационной безопасности и защиты информации для интеллектуальных систем транспорта. Разработана информационная технология и система поддержки принятия решений для определения степени защиты интеллектуальных систем транспорта. Метод позволяет повысить эффективность распознавания угроз для информационной безопасности интеллектуальных систем транспорта, а также создавать более эффективные системы защиты информации на транспорте.

Ключевые слова: интеллектуальные транспортные системы, защита информации, информационная безопасность, распознавание угроз, нечеткие множества.

INFORMATION SECURITY OF INTELLECTUAL TRANSPORT SYSTEMS

This paper contains research results aimed at further development of models for information and communication environment, intellectual transport systems threat detection and information security improvement in the emerging unified information-communication environment, implementation of new and upgrading existing information systems in transport and increase the number of destabilizing effects on the availability, confidentiality and integrity of information. The analysis of traditional methods of solving this task is conducted. The construction method of linear on parameters regressive mechanism of inference is offered for a consulting model with fuzzy data's. Offered diagnostic model and the algorithm provides more precise determining of parameters of information security, which will result in increasing of level of protection of intellectual transport systems.

Keywords: intelligent transportation systems, information security, information security, threat detection, fuzzy sets.

Лахно Валерий Анатольевич, доктор технических наук, доцент, заведующий кафедры организации комплексной защиты информации Европейского университета.
E-mail: valss21@ukr.net.
Лахно Валерій Анатолійович, доктор технічних наук, доцент, завідувач кафедри організації комплексного захисту інформації Європейського університету..
Lakhno Valery, Doctor of Science**,** associate professor, Head of Complex Information Security Organization Department, European University (Kyiv, Ukraine).