УДК 004.056.53:656.078

В.А. Лахно

МОДЕЛІ, МЕТОДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ СИСТЕМ ТРАНСПОРТУ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ ЗАГРОЗ

Анотація. Робота містить результати досліджень направлених на подальший розвиток методів та моделей інтелектуального розпізнаванні загроз інформаційно-комунікаційному середовищу транспортної галузі (ІКСТГ) та удосконаленню інформаційної безпеки (ІБ) в умовах формування єдиного інформаційно-комунікаційного середовища, створення державної єдиної інтегрованої інформаційної системи (ДЄІІС), впровадження нових та модернізації існуючих інформаційних систем на транспорті, і збільшення кількості дестабілізуючих впливів на доступність, схоронність і цілісність інформації. Розроблено метод інтелектуального розпізнавання загроз на основі дискретних процедур з використанням апарату логічних функцій та нечітких множин, що дозволяє підвищити ефективність розпізнавання загроз ІКСТГ, створювати ефективні аналітичні, схемотехнічні та програмні рішення СЗІ ІКСТГ.

Ключові слова: захист інформації, інформаційна безпека, інтелектуальне розпізнавання загроз, дискретні процедури, нечіткі множини, неоднорідні потоки даних, транспортна галузь.

Вступ

Інформаційні технології та системи, що розвиваються в транспортній галузі (ТГ), активно орієнтовані на взаємодію із системами інших секторів економіки для скорочення затримок при транспортуванні вантажів, обробці морських та річкових суден, контейнерів, залізничних вагонів і автофургонів на прикордонних переходах, мультимодальних логістичних центрах, на основі використання даних електронних накладних, систем клієнт-банк, e-business, e-logistics, e-cargo, e-ticket, взаємодії із клієнтурою й партнерами тощо.

В рамках державних і міждержавних програм інформатизації створюються сучасні комплекси інформаційних, інформаційно-керуючих та автоматизованих інформаційних систем транспортної

© Лахно В.А., 2014

галузі (далі по тексту ІСТГ), а також державна єдина інтегрована інформаційна система (ДЄІІС).

Активне розширення інформаційно-комунікаційного середовища транспортної галузі (ІКСТГ), особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується появою нових загроз інформаційній безпеці (ІБ), про що свідчить статистика інцидентів, див. рис. 1.

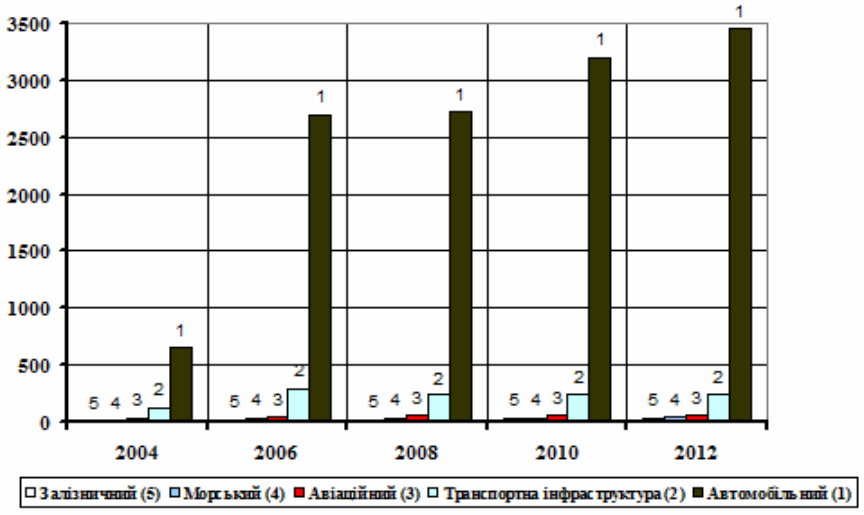

Рисунок 1 - Загальна кількість інцидентів із ІБ на транспорті

Дослідженнями ІБ ТГ присвячені роботи: Алексєєва В.О., Бабака В.П., Бірюкова Д.С., Блінцова В.С., Вільського Г.Б., Єсікова О.В., Корнієнко О.О., Корченко О.Г., Риндюка В.А., Стасюка О.І., Харченка В.П. та ін. Однак в Україні ці дослідження носять фрагментарний характер [1, 2, 3]. Завдання визначення ризиків нападу на інформаційні ресурси транспортного сектору економіки, та ІСТГ, зокрема, належним чином не розглядається та, у найкращому випадку, підмінюється на етапі проектування систем захисту інформації якісним аналізом надійності системи й можливих наслідків проникнення до неї [2, 3].

Отже, актуальність досліджень, спрямованих на подальший розвиток моделей та методів захисту на основі інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту та забезпечення ІБ галузі в умовах створення державної єдиної інтегрованої інформаційної системи, є однією з ключових проблем захисту інформації об'єктів критичної інфраструктури держави.

Постановка завдання. У зв'язку із цим **мета статті** полягає у викладенні методу та моделей розпізнавання загроз інформаційній безпеці, які, на відміну від існуючих, дозволяють прийняти остаточне рішення про наявність або відсутність загрози в межах існуючих та нових класів вторгнень у ІСКТГ.

Метод інтелектуального розпізнаванні загроз

Ступінь небезпеки кожної загрози ІКСТГ залежить від значень ряду факторів, що підвищують або знижують захищеність об'єкту інформаційної безпеки (ОІБ) від загрози певного класу, наприклад комп'ютерного вторгнення. Фактори, що знижують захищеність ОІБ, будемо називати факторами ризику, а ті, що підвищують її - факторами захищеності. Інтегральна оцінка уразливості й захищеності ОІБ є функцією його захищеності від кожного виду загроз. Інформація, яка є основою побудови ДПРЗ ІБ може бути подана в різних формах, зокрема, у вигляді важко з'ясовних ознак НСД $\{p_{ax1},...,p_{axn}\}$ у ДЄІІС та ІСТГ, діапазонів граничних значень, параметрів вхідного вихідного трафіка, непередбачуваних адрес пакетів, атрибутів, часових параметрів, запитів і т. д.

В роботі досліджена множина об'єктів PA - число можливих цілей порушника в ІКСТГ. Об'єкти цієї множини описуються системою ознак $\{p_{ax1},...,p_{axn}\}$. Множина PA представлена у вигляді об'єднання непересічних підмножин (класів) загроз ІБ - $(KL_1,...,KL_l)=(B_{p_{a1}},...,B_{p_{al}})$, де B_{p_a} - множина номерів загроз ІКСТГ, реалізованих порушником при досягненні p_a - i мети.

Існує остаточний набір об'єктів $\{sp_{a1},...,sp_{am}\}$ з PA, про які відомо, до яких класів загроз вони належать (це прецеденти, тобто об'єкти, використовувані для навчання - ОВН). Потрібно за пред'явленим набором значень ознак, тобто описом деякого об'єкта sp_{an} з PA, про який невідомо, до якого класу він належить, визначити цей клас і, відповідно, вибудувати роботу СЗІ таким чином, щоб вона могла ефективно протидіяти загрозі в межах даного класу.

Головною особливістю запропонованого методу інтелектуального розпізнавання загроз ІКСТГ, є можливість одержання результату за відсутності інформації про функції розподілу значень ознак і за наявності малих навчальних вибірок.

Основним завданням побудови ДПРЗ є пошук інформативних підописів (або фрагментів описів) об'єктів, див. табл. 1.

Інформативними вважаються фрагменти, які відображають певні закономірності в описах об'єктів, використовуваних для навчання. У ДПРЗ ІБ інформативними вважаються такі фрагменти, які зустрічаються в описах об'єктів одного класу, але не зустрічаються в описах об'єктів інших класів загроз ІБ. Розглянуті фрагменти, зазвичай, мають змістовний опис у термінах проектування СЗІ ІКСТГ.

При побудові ДПРЗ ІБ введено поняття елементарного класифікатора, під яким розуміють фрагмент опису об'єкта, використовуваного для навчання (ОВН). Для кожного класу загроз ІБ $(KL_1,...,KL_l)=(B_{p_{a1}},...,B_{p_{al}})$ будується множина елементарних класифікаторів із заздалегідь заданими властивостями та, як правило, використовуються класифікатори, які зустрічаються в описах об'єктів одного класу й не зустрічаються в описах об'єктів інших класів, тобто характеризують лише деякі з ОВН даного класу загроз ІБ.

Таблиця 1

База знань для інтелектуального розпізнавання загроз ІКСТГ

Класи загроз ІБ			Атрибути (Ознаки класу загроз)		Ознаки $\{p_{ax1},...,p_{axn}\}$	Інформативність ознаки	Універсум	Терми для лінгвістичної оцінки
Можливі загрози ІБ ІКСТГ	Відомі загрози		KL_1	Відмова у обслуговуванні	……	$IZ_{p_{axj}}$	[0,1], у. о.	некритичний (нкр), критичний (кр)
			KL_2	Викрадення інформації	……	$IZ_{p_{axj}}$	[0,1], у. о.	виявлені (в), частково невиявлені (чв), невиявлені (нв)
			…	……	……	……	……	……
			KL_{MI}	……	……	……	……	……
	Невідомі загрози	Описані	KLO_{21} – KLO_{2n}	……	……	……	……	……
		Неописані	KLN_{31} – KLN_{3m}	……	……	……	……	……

Таким чином, модель інтелектуального розпізнавання загроз ІКСТГ, виглядає наступним чином.

1. У системі ознак $\{p_{a_1},...,p_{a_{jMI}}\}$ виділяється сукупність різних підмножин виду $NP_{p_a}=\{p_{aj_1},...,p_{a_{MI}}\}$, $r_{p_a} \le MI$.

 ISSN 1562-9945

2. Виділені підмножини називаються опорними множинами, а вся їхня сукупність позначається через ΩMI.

3. Задаються параметри: po_{sp_a} - параметр, що характеризує значущість мети (об'єкта) sp_{ai}, i=1, 2,..., PA; $po_{NP_{pa}}$ - параметр, що характеризує значущість об'єкта опорної множини $NP_{p_a} \in \Omega MI$.

4. Виконується процедура обчислення оцінок. Розпізнаваний об'єкт вторгнення sp_{an} порівнюється з кожним ОВН sp_{ai} за кожною опорною множиною.

5. Для кожного класу загроз ІКСТГ KL, $KL \in \{KL_1,...,KL_l\}$, обчислюється оцінка приналежності $\Gamma(sp_a, KL)$ об'єкта sp_a до класу KL, яка має вигляд:

$$\Gamma(sp_a, KL) = \frac{1}{|LW_{KL}|} \sum_{sp_{ai} \in KL} \sum_{NP_{p_a} \in \Omega MI} po_{sp_a} \cdot po_{NP_{pa}} \cdot BN(sp_a, sp_{ai}, NP_{p_a}), \qquad (1)$$

де $|LW_{KL}| = |KL \cap \{sp_{a1},...,sp_{aMI.}\}|$.

Об'єкт sp_{an} належить до того класу, який має найбільшу оцінку.

6. Якщо класів з найбільшою оцінкою небагато, то відбувається відмова від розпізнавання. Для коректності цього алгоритму отримана наступна система лінійних нерівностей:

$$\Gamma(\mathrm{sp}_{a1}, KL_1) > \Gamma(\mathrm{sp}_{a1}, KL_2),\ \Gamma(\mathrm{sp}_{aMI_1}, KL_1) > \Gamma(\mathrm{sp}_{aMI_1}, KL_2),\ \Gamma(\mathrm{sp}_{aMI_{1+1}}, KL_2) > \Gamma(\mathrm{sp}_{aMI_{1+1}}, KL_1).$$

. . .

$$\Gamma(\mathrm{sp}_{aMI}, KL_2) > \Gamma(\mathrm{sp}_{aMI}, KL_1).$$

Рішення системи зводиться до вибору параметрів $po_{sp_{ai}}$ i = 1, 2,..., PA, та $po_{NP_{pa}}$, $NP_{p_a} \in \Omega MI$. У разі, якщо система несумісна, знаходиться її максимальна спільна підсистема й з рішення цієї підсистеми визначаються значення параметрів $po_{sp_{ai}}$ і $po_{NP_{pa}}$.

Процедура розпізнавання загрози ІКСТГ для об'єкта $sp_a = (\alpha p_{a1},...,\alpha p_{aMI})$, здійснюється на підставі розрахунків за побудованими елементарними кон'юнкціям. Показано, що найбільш економічним є використання алгоритму розрахунків кон'юнкцій за покриттями класу загроз ІБ ІКСТГ. Характеристична функція класу загроз ІБ KL_l - певна логічна функція F_{KL}, що ухвалює значення 0 на описах об'єктів $sp_{an} = (\alpha p_{an1},...,\alpha p_{anMI})$ з KL_l і значення 1 на інших набо-

рах з E_{KL}^{MI}, тут E_{KL}^{MI} - множина усіх наборів довжини r_{p_a}. Покриттю класу KL_l відповідає припустима для $F_{\overline{KL}}$ кон'юнкція, тупиковому покриттю - максимальна для $F_{\overline{KL}}$ кон'юнкція. Припустима (максимальна) кон'юнкція $\Re$ визначає приналежність об'єкта $sp_{an}=(\alpha p_{an1},...\alpha p_{anMI})$ класу $(KL_l)=(B_{p_{al}})$, якщо $(\alpha p_{a1},...,\alpha p_{aMI})\notin NI_{\Re}$.

Побудувати скорочену ДНФ логічної функції можна також шляхом перетворення кон'юнктивної форми вигляду $D_1 \wedge D_2 \wedge ... \wedge D_u$, де $D_i = p_{ax1}^{\overline{\beta_{i1}}} \vee p_{ax2}^{\overline{\beta_{i2}}} \vee ... \vee p_{axMI}^{\overline{\beta_{iMI}}}, i=1,2,..,mu$ реалізує функцію F_{KL}, β_{iMI} - елементи набору $B_{F_{\overline{KL}}}$, де $\overline{p_{ax}^{\alpha}} = \bigvee\limits_{\beta_i \neq \alpha_i} p_{ax}^{\beta}$.

Тоді кон'юнктива форма набуває вигляду $D^*_1 \wedge D^*_2 \wedge ... \wedge D^*_u$, де $D^*_i = \bigvee\limits_{\iota \neq \beta_{i1}} p_{ax1}^{\eta} \vee \bigvee\limits_{\iota \neq \beta_{i2}} p_{ax2}^{\eta} \vee ... \vee \bigvee\limits_{\iota \neq \beta_{iMI}} p_{axMI}^{\eta}, i=1,2,..,u.$

Таким чином, побудова множини елементарних класифікаторів для модельованого класу загроз ІКСТГ зводиться до такого: 1) задається характеристична функція; 2) будується ДНФ, що реалізує цю функцію. 3) обчислюється припустима (максимальна) кон'юнкція $\Re$, що визначає приналежність об'єкта до певного класу загроз ІКСТГ.

Для кожного класу кількість ознак варіювалася від 3 до 9. Інформативність ознаки змінювалася в діапазоні від -1 до +1. Для оцінки ефективності процедур розпізнавання використовувався метод ковзного контролю.

Приклади результатів тестування продуктивності методу ДПРЗ показані на рис. 2-5.

Рисунок 2 - Ймовірність розпізнавання загрози «НСД до відеосервера»

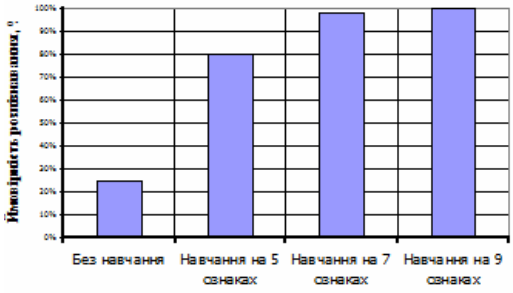

Рисунок 3 - Ймовірність розпізнавання загрози «НСД до пароля користувача»

 ISSN 1562-9945

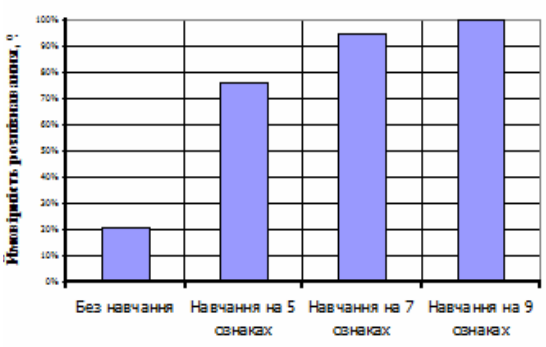

Рисунок 4 - Ймовірність розпізнавання загрози «НСД до ПЗ та БД ІС ТГ»

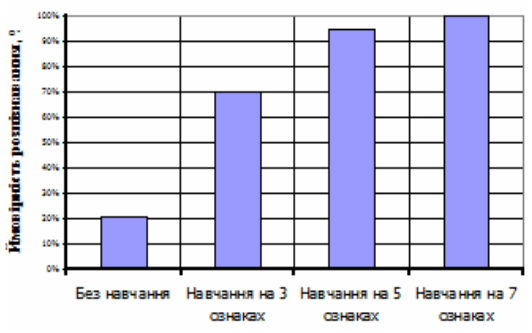

Рисунок 5 - Ймовірність розпізнавання загрози «НСД до систем супутникової навігації»

Для подальшого розв'язання проблеми розвитку моделей інтелектуального розпізнавання загроз ІКСТГ, потрібно зосередитися на розгляді режимів роботи ДЄІІС та ІСТГ у разі втрати заявок внаслідок блокування неоднорідних потоків ДПРЗ, які виникають при складних вторгненнях у ІКСТГ, або коли втрати з'являються через переповнення заявками у відповідних модулях підсистем клієнт-банк, електронних накладних, e-business, e-logistics, e-cargo, e-ticket, систем GSM-R, VSAT та ін.

Модель інтелектуального розпізнавання загроз ІКСТГ в умовах неоднорідних потоків запитів при DDoS атаках

В даний час існує багато робіт, що розкривають різні підходи до моделювання інформаційних вторгнень: мережі Петрі, метод аналізу зміни станів, емуляція вторгнень в послідовному і паралельному режимах, концептуальні моделі комп'ютерних вторгнень, описові моделі мережі і зловмисників та інші [1-4].

Теоретичним підґрунтям таких моделей ПБ служить так звана основна теорема безпеки, яка формулюється і доводиться окремо для кожної моделі.

Дискреційна модель, що встановлює повноваження доступу користувачів, найбільше підтримує глобальну ПБ. Однак, вона є принципово не безпечною.

У цьому зв'язку актуальна розробка моделей розпізнавання загроз, які є моделями кінцевих станів по суті і дискреційними за формою.

Позначимо через N_A – множину номерів загроз ІБ ДЄІІС та ІСТГ; $D_{сзі}$ – множину номерів засобів захисту (ЗЗІ), які можуть бути

використані в СЗІ ДЄІІС та ІСТГ; B_{p_a} - множину номерів загроз ІБ, реалізованих порушником при досягненні p_a -ої мети; $N_j^{p_a}$ -множину номерів ЗЗІ, які потенційно можуть бути використані для протидії реалізації порушником p_a - ої мети на j-*му* рубежі захисту (для нейтралізації *j*-ї загрози, що входить в p_a-у ціль) (p_a=*1,2,...,PA; j=1,2,...,MI*). Причому, $B_{p_a} \subset N_A$, $\bigcup_{p_a=1}^{PA} B_{p_a} = N_A$, $n_{p_a} = \left|B_{p_a}\right|$ і $\bigcup_{p_a=1}^{PA} \bigcup_{j \in B_{p_a}}^{n_{p_a}} N_j^{p_a} \subset D_{сзі}$. В цьому випадку процес реалізації порушником кожної зі своїх цілей може бути представлений у вигляді спрямованого графа, див. рис. 6.

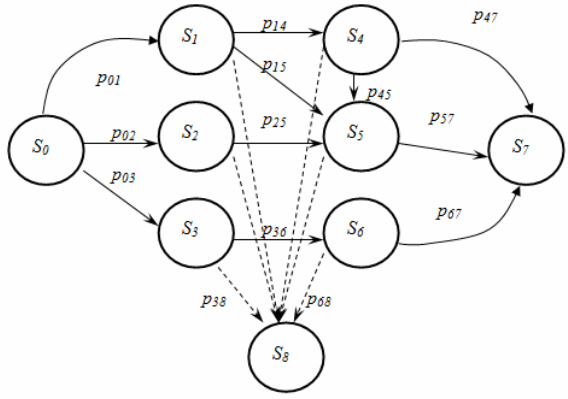

Рисунок 6 - Граф станів ДЄІІС та ІСТГ

Відповідно до запропонованого методу інтелектуального розпізнавання загроз, складемо базу знань для процедури складання вирішального правила при вторгненнях типу «Відмова у обслуговувані» при неоднорідних потоках запитів у ДЄІІС та ІС ТГ, див. табл. 2.

Для тестування продуктивності ДПРЗ та розробленої експертної системи, (див. рис. 7) обрана задача зіставлення загрозам DoS/DDoS вторгнень відомих методів захисту. База знань із 9 правил розрізняє 7 типів атак DoS/DDoS на основі відомих ознак, вхідних і додаткових атрибутів, що описують поточний стан системи (табл. 1,2).

Для кожного із співвідношень виду $D = f(\phi_i \vee y_1 \vee .. y_n)$, які описують певну тактику захисту від вторгнення, 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.

 ISSN 1562-9945

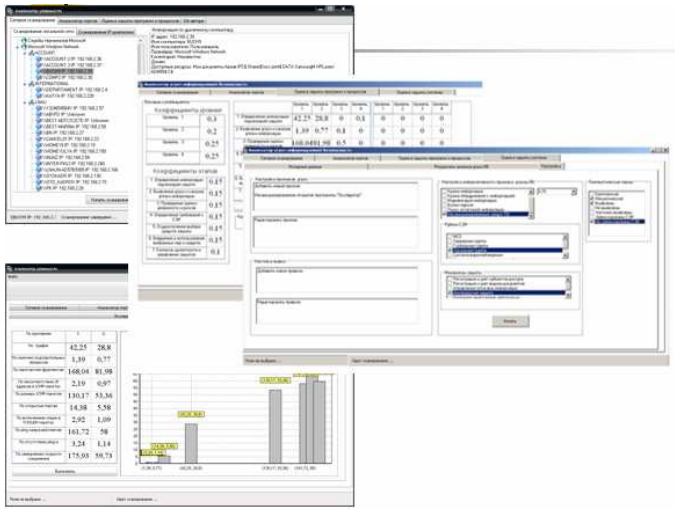

Рисунок 7 - Загальний вид програми «Аналізатор загроз»

Таблиця 2

Ознаки при DDoS та DoS атаках у ІКСТГ

Частковий параметр стану ІС	Універсум	Терми для лінгвістичної оцінки
ϕ_1 – інтенсивність потоку кадрів (запитів), що поступають к серверам ІС	[10,6000], кадр/с	немає (н), незначна кількість (нк), середня кількість (ск), велика кількість (вк)
ϕ_2 – номінальна пропускна спроможність середовища передачі даних ІС	[10,100], Мбіт/с	низка (нпс), середня (спс), велика (впс)
….	….	….
ϕ_{13} - наявність HTTP GET пакетів	[0,1], у. о.	мала кількість (м), середня (с), велика (в)
ϕ_{14} -наявність HTTP flood пакетів	[0,1], у. о.	мала кількість (м), середня (с), велика (в)
….	….	….
ϕ_z - інші фактори		

Наприклад, скорочено систему логічних рівнянь, що відповідає співвідношенню для інтелектуального розпізнавання низькоактивних DDoS-атак прикладного рівня («повільний» HTTP GET flood і «повільний» HTTP POST flood), запишемо так:

$$\mu^{d_j}(\mathrm{S}) = \bigvee_{p=1}^{h_j}\left[\mu^{y_1^{jp}}(y_1)\wedge\mu^{\phi_я^{jp}}(\phi_{13})\wedge\mu^{\phi_я^{jp}}(\phi_{14})\right],\ p=\overline{1,h_j}\ ,\ j=\overline{1,M}\ , \qquad (2)$$

де $\mu^{y_1^{jp}}(y_1)$, $\mu^{\phi_я^{jp}}(\phi_{13})$, $\mu^{\phi_я^{jp}}(\phi_{14})$ – функції належності змінних y_1 , ϕ_{13}, ϕ_{14} до їх нечітких термів y_1^{jp} , ϕ_{13}^{jp} , ϕ_{14}^{jp} відповідно; S – стан захисту ІСТГ від атак DoS/DDoS; y_1 – стан ІБ {нижче за критичний (нкр), критичний (кр), вище за критичний (вкр), високий (в)}; $\vee$ – логічне АБО, $\wedge$ – логічне І, як операції *max* і *min* відповідно.

На рис. 8 показані основні результати, отримані в ході тестового моделювання процедури розпізнавання атак DoS/DDoS на ДЄІІС та ІСТГ.

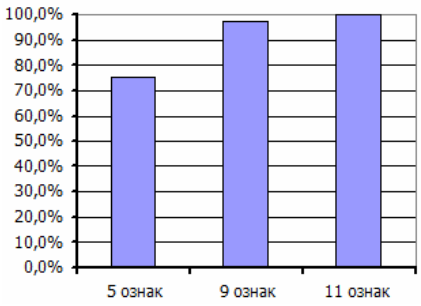

Рисунок 8 - Ймовірність виявлення DDoS-атак

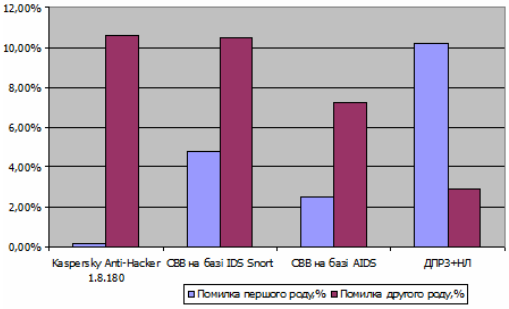

Рисунок 9 - Значення помилок виявлення DDoS-атак першого роду і другого роду для різних систем

В результаті означеного експерименту для розробленого методу інтелектуального розпізнавання DDoS/DDoS - атак були отримані наступні результати для помилок першого роду (кількість помилкових спрацьовувань) - 10,2%) і помилок другого роду (кількість невиявлених атак) - 2,9%, див. рис. 9.

Висновки

Робота присвячена дослідженню та розвитку теоретичних і методологічних питань захисту інформації у транспортній галузі України, розробці методів, моделей та програмних продуктів для забезпечення ІБ на транспорті в умовах формування єдиного інформаційно-комунікаційного середовища, створення державної єдиної інтегрованої інформаційної системи, впроваджені нових та модернізації існуючих ІСТГ, і збільшення кількості дестабілізуючих впливів на схоронність і цілісність інформації.

Основні результати досліджень полягають у такому:

 ISSN 1562-9945

1. Розроблено метод інтелектуального розпізнавання загроз на основі дискретних процедур з використанням апарату логічних функцій та нечітких множин, що дозволяє підвищити ефективність розпізнавання загроз ІКСТГ в залежності від класу до 85-98 %, створювати ефективні аналітичні, схемотехнічні та програмні рішення СЗІ ІКСТГ.

2. Удосконалено моделі інтелектуального розпізнавання загроз ІКСТГ в умовах реалізації комп'ютерних вторгнень «Відмова у обслуговуванні», з урахуванням можливостей зміни нападаючим інтенсивності неоднорідних потоків запитів. Запропоновані моделі, доведені до практичної реалізації шляхом створення відповідних програмних модулів, що дозволяє підвищити ефективність розпізнавання комп'ютерних вторгнень «Відмова у обслуговуванні» до 97-98 %.

ЛИТЕРАТУРА

1. Вильский Г.Б. Информационные риски судовождения / Г.Б. Вильский // Наук. Вістник ХДМА - № 1(4) / Херсон: ХДМІ, 2012. - С.17-26.
2. 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.
3. Корниенко А.А. Средства защиты информации на железнодорожном транспорте. [учебное пособие] / Корниенко А.А. М.А. Еремеев, С.Е. Ададуров - М.: Маршрут. – 2006, 256 с.
4. Лахно В.А. Компьютерное моделирование DoS атаки на серверы компьютерных систем. / Лахно В.А., Петров А.С. // Сучасна спеціальна техніка. Науково-практичний журнал №2(25), 2011. С. 81-89.
5. 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.