***Для підвищення інформаційної безпеки транспортних систем необхідно проводити дослідження, які спрямовані на подальший розвиток методів та моделей розпізнаванні кіберзагроз інформаційно-комунікаційному середовищу транспорту (ІКСТ) та прийняття рішень при нечітко заданій вхідній інформації. Запропонований новий підхід прийняття рішень для забезпечення кібербезпеки інформаційних систем наземного транспорту. Розглянуто випадок кіберзахисту ІКСТ на основі нечіткого регресійного механізму логічного висновку для системи підтримки прийняття рішень з нечіткими початковими даними***

***Ключові слова: інформаційно-комунікаційне середовище транспорту, кібербезпека, захист інформації, розпізнавання загроз***

***Для повышения информационной безопасности транспортных систем необходимо проводить исследования, направленные на дальнейшее развитие методов и моделей распознавании киберугроз информационно-коммуникационной среде транспорта (ИКСТ) и принятия решений при нечетко заданной входной информации. Предложен новый подход принятия решений для обеспечения кибербезопасности информационных систем наземного транспорта. Рассмотрен случай киберзащиты на основе нечеткого регрессионного механизма логического вывода для системы поддержки принятия решений с нечеткими исходными данными***

***Ключевые слова: информационно-коммуникационная среда транспорта, кибербезопасность, защита информации, распознавания угроз***

УДК 004.056.53:656.078
DOI: 10.15587/1729-4061.2016.60711

# ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ТРАНСПОРТУ В УМОВАХ ДЕСТРУКТИВНОГО ВПЛИВУ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

**В. А. Лахно**
Доктор технічних наук, доцент
Кафедра організації комплексного захисту інформації*
E-mail: lva964@gmail.com
**А. В. Грабарєв**
Кандидат економічних наук, декан
Факультет інформаційних систем та технологій*
E-mail: andr.grab@gmail.com
*Європейський університет
бул. Академіка Вернадського, 16В,
м. Київ, Україна, 03115

## 1. Вступ

В умовах євроінтеграції України стрімко зростає роль транспортної галузі у забезпеченні розвитку торгово-економічних відносин між нашою державою та країнами ЄС, їх туристичних, культурних, та спортивних зв'язків. Участь України в міжнародних інтеграційних бізнес процесах на транспорті безальтернативна, але вона повинна супроводжуватися створенням сучасної інформаційно-комунікаційної інфраструктури, сумісної з інфраструктурою країн, з якими Україна взаємодіє, з одночасним забезпеченням захисту національних інтересів, зокрема у питаннях забезпечення кіберзахисту інформаційно-комунікаційних систем транспорту (ІКСТ).

Активне розширення ІКСТ, особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується виникненням нових загроз для інформаційної безпеки (ІБ), про що свідчить зростання кількості інцидентів, пов'язаних із кібербезпекою та захистом інформації на транспорті. Кіберзагрози для ІКСТ є цілком реальними, оскільки злочинці можуть отримати можливість перехоплювати паролі, окремі файли, геолокаційну інформацію, транслювати аудіо- та відеодані, контролювати бездротові мережі, веб-камери, інформаційні табло на автомобільних і залізничних шляхах, вокзалах, аеропортах та ін.

Отже, актуальність нових досліджень, спрямованих на подальший розвиток методів захисту на основі інтелектуального розпізнавання кіберзагроз ІКСТ та забезпечення ІБ галузі, є однією з ключових проблем кіберзахисту об'єктів критичної інфраструктури держави.

## 2. Аналіз літературних даних і постановка проблеми

Всеосяжний характер завдань формування ІКСТ вимагає їх систематизації, вибору пріоритетів, зокрема, такими пріоритетами є: розширення сфери надання транспортних послуг; забезпечення їх більшої доступності для суб'єктів економічної діяльності та населення [1]; підвищення якості транспортних послуг

[2], а також, підвищення рівня безпеки транспорту, в тому числі, інформаційної складової, за рахунок застосування комплексних інформаційно телекомунікаційних (ІТК) та телематичних систем контролю, моніторингу, управління та ін. [3].

Для України питання захисту інформації та забезпечення інформаційної безпеки транспортної галузі (ТГ) мають особливе значення. Це пов'язано, насамперед, з розмірами території та геополітичним розташуванням нашої країни, з політичним і соціально-економічним курсами, спрямованими на подальше зміцнення суверенітету.

Проблеми, пов'язані із захистом інформації й забезпеченням кібербезпеки транспорту, успішно вирішують провідні українські та закордонні вчені [4–10].

Однак ці публікації носять фрагментарний характер. Так, в одних джерелах представлені теоретичні дослідження [4, 5], в інших опис апаратних і програмних засобів забезпечення кібербезпеки [6, 7], або результати експериментів [8, 9]. Також, на жаль, визначення загроз для транспортної безпеки, зокрема її інформаційної складової [10, 11] в цих роботах не наведено. Більш того, більшість робот розглядають проблеми кіберзахисту окремо по кожному виду транспорту, залізничному [12, 13], авіаційному [10], морському [11] або автомобільному [9]. Отже, транспортна галузь в цілому в цих роботах не розглядається. Також зазначимо, що інформаційна безпека ТГ ніколи не виділялася в якості самостійного виду національної безпеки. Більше того, ІБ транспортної галузі (ІБ ТГ) не може існувати поза рамками національної безпеки. Як частина єдиного цілого, вона несе в собі спадковість концептуальних підходів щодо забезпечення безпеки країни на мікро- і макрорівнях, нерозривність взаємозв'язків, спільність принципів і методів. Причому кібербезпека на транспорті об'єктивно має свої особливості і специфіку, що відображає галузеву спрямованість і визначальне її місце, роль і значення в структурі національної безпеки [9–11].

## 3. Мета і завдання дослідження

Метою даної роботи є апробація методу інтелектуального розпізнавання кібератак на основі дискретних процедур для побудови адаптивних систем кіберзахисту інформаційно-комунікаційних систем транспорту, в умовах збільшення кількості дестабілізуючих впливів на схоронність, доступність і цілісність інформаційних ресурсів транспортної галузі.

Для досягнення поставленої мети були поставлені наступні завдання:

– проаналізувати можливість створення захищеного ІКСТ, адаптованого до умов формування єдиного інформаційно-комунікаційного простору, створення та модернізації сучасних ІС та АСК за збільшення кількості дестабілізуючих впливів на кібербезпеку транспорту;

– розробити метод інтелектуального розпізнавання кіберзагроз на основі дискретних процедур для забезпечення інформаційної безпеки ІКСТ на основі комплексного застосування існуючих засобів і методів захисту інформації в інтересах підтримки стійкої працездатності ІС та АСК ТГ.

## 4. Захист інформаційно-комунікаційного середовища транспорту як складова системи національної безпеки

Втручання в національні, регіональні й муніципальні автоматизовані інформаційні та інформаційно-керуючи системи на транспорті часто згадувана загроза для кібератак зловмисників [10–12]. Але, ми ще не перебуваємо на тому рівні, коли бізнес-процеси на транспорті залежать винятково від комп'ютерних мереж. При цьому комунікації, які використовуються в інформаційно-комунікаційних системах транспорту (ІКСТ), можуть і не залежати від Інтернету. Високий ступінь залучення людини до транспортної логістики та керування процесами транспортування зменшують ризик кібератак. Але статистика інцидентів з інформаційною безпекою на транспорті поповнюється кожен рік, рис. 1.

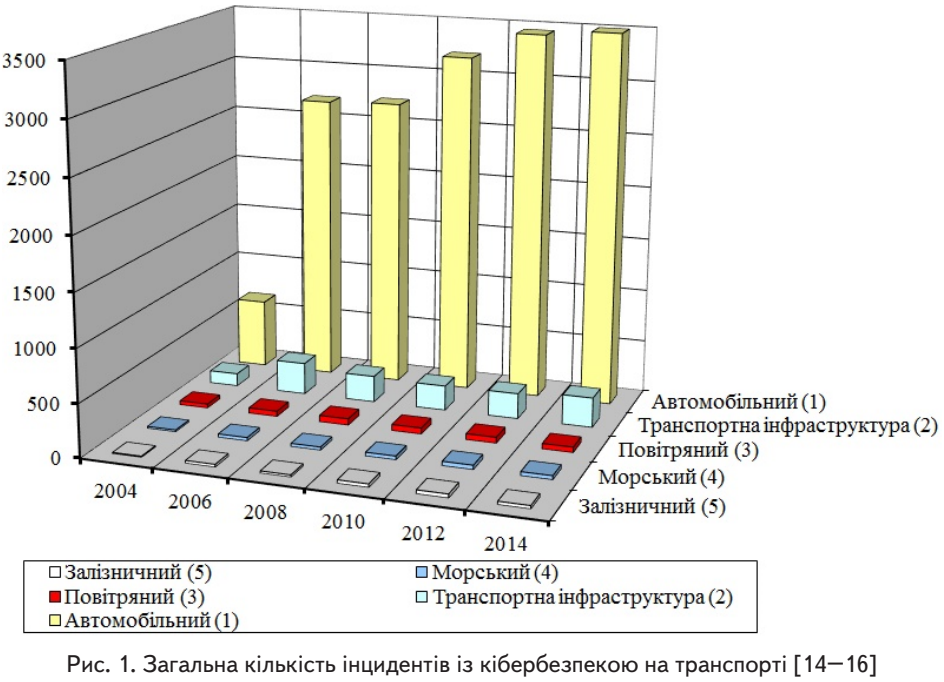


Рис. 1. Загальна кількість інцидентів із кібербезпекою на транспорті [14–16]

Разом із тим, завдання визначення ризиків нападу на інформаційні ресурси транспортного сектору економіки, та ІСТГ, зокрема, належним чином не розглядається та, у найкращому випадку, підмінюється на етапі [4, 10] проектування систем захисту інформації якісним аналізом надійності системи й можливих наслідків проникнення до неї [13].

Для будь-яких ІКСТ характерними є наступні види елементів: бортові засоби [10, 11], що встановлюються на рухомі об'єкти (засоби дистанційного моніторингу, виміру і т. п.); засоби, що встановлюються на стаціонарні об'єкти інфраструктури (засоби дистанційного моніторингу, виміру і т. п.); дистанційно керовані виконавчі та індикаційні пристрої (прилади, вузли та агрегати); сервери для обробки та зберігання інформації [13]; ситуаційні, диспетчерські та оперативні центри [9–13]; засоби забезпечення зв'язку – Інтернет, мережа GSM/GPRS, GSM-R, VSAT, супутниковий зв'язок [9]; інформаційно-телекомунікаційні засоби, що забезпечують захищену інформаційну взаємодію із зовнішніми інформаційними системами.

Інтерес для зловмисників можуть представляти такі складові автоматизованих систем керування (АСК), як системи SCADA і людино-машинного інтерфейсу (HMI), в яких в період з 2004 р. по 2013 р. було виявлено більше 120 уразливостей. Майже третина уразливостей (36 %) пов'язана з переповненням буфера – явищем, що виникає, коли комп'ютерна програма записує дані за межами виділеного в пам'яті буфера. Подібний недолік захищеності дозволяє зловмисникові не тільки викликати крах або «зависання» програми (відмова в обслуговуванні), але й виконувати в цільовій системі довільний код. Якщо скласти всі типи уразливостей, експлуатація яких дозволяє хакеру запустити виконання стороннього коду або викликати відмову в обслуговуванні (Buffer Overflow, Remote Code Execution, DoS), то вийде близько 50 % всіх уразливостей [16–18].

За даними, представленими в [16–18] кількість уразливостей в АСК зв'язку та транспорту, з 2004 року збільшилися на 600 %, рис. 2.

Крім того, як показало дослідження [17], вимоги до рівня складності для успішного проведення атаки проти промислових та транспортних систем, а також систем зв'язку (після того як зловмисник отримав доступ до цілі кібератаки), частка уразливостей низької складності знизилася з максимального рівня – більш ніж на 90 % в 2004 році, до 48 % в 2012 році. Тим часом, за той же період уразливості середньої складності збільшили свою частку з 5 % до 47 %, рис. 3. Розкриття інформації зі складними уразливими залишалося стабільним в останні десятиліття, їх частка в середньому становить всього 4 % [16, 17].

У зловмисників є кілька точок входу, щоб скомпрометувати АСК або інформаційні системи (ІС). ІКСТ 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 [14, 15, 17], тобто, це в вісім разів більше, ніж за період з 2005 р. по 2010 р.

Порушення працездатності ІС або АСК може призвести до серйозних збоїв і значного збитку, проте розробники таких систем все ще приділяють недостатньо уваги захищеності своїх продуктів, що демонструється на щорічних конкурсах Choo Choo Pwn (Південна Корея). Так, наприклад, в 2013 і 2014 року учасники повинні були знайти і скористатися уразливими в АСК і отримати доступ до системи управління моделлю залізниці, а також, порушити працездатність автоматичного залізничного переїзду. АСК моделлю залізниці була побудована на продуктах компанії Siemens і контроллерах S7-1200. У ході конкурсу вдалося відправити системі помилкові сигнали та в ході спуфинга АСК перестала працювати (DoS) [15].

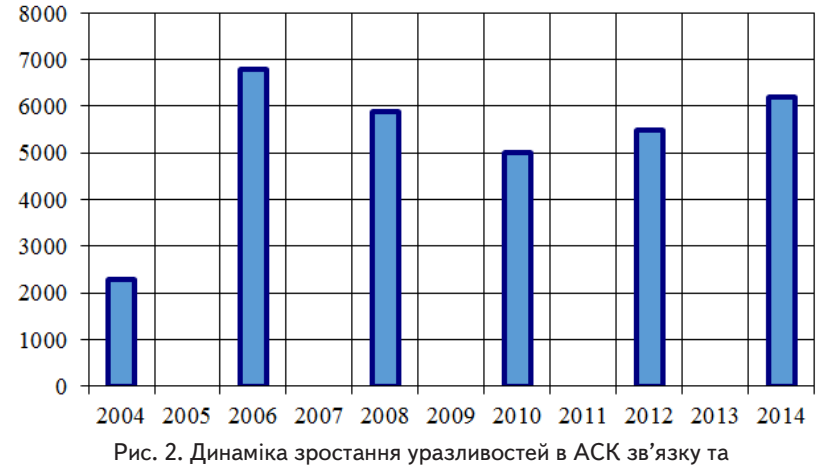


Рис. 2. Динаміка зростання уразливостей в АСК зв'язку та транспорту [14, 15, 17, 18]

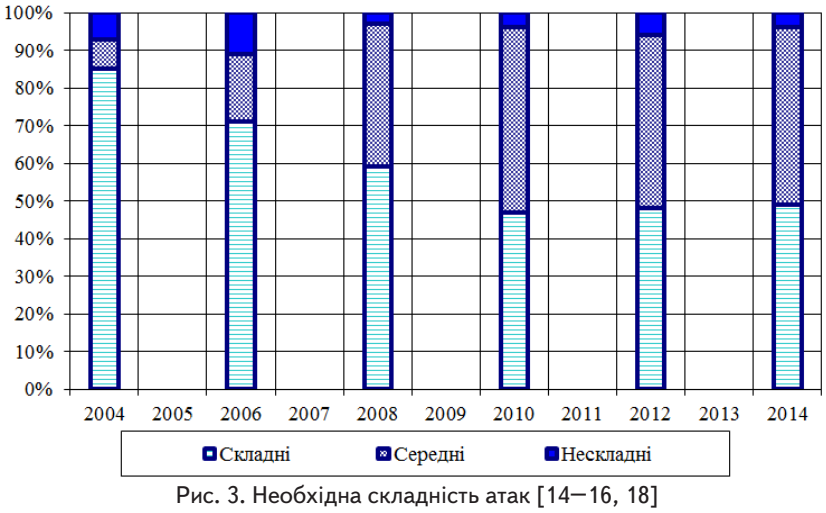


Рис. 3. Необхідна складність атак [14–16, 18]

Уразливість АСК, SCADA, HMI, PLC 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 – операційної системи, мережевих протоколів і служб, віддаленого доступу – теж не сприяють безпеці АСК.

## 5. Метод інтелектуального розпізнавання кіберзагроз ІКСТ

Критичність виходу з ладу ІКСТ вимагає опрацювання питань захисту інформації та забезпечення ІБ з акцентом на доступність та стійкість системи, а також цілісність інформації.

Наприклад, можливі два підходи до побудови периметрів забезпечення кібербезпеки єдиного інформаційного центру (ЄІЦ) ТГ – на основі рівнів або вимог безпеки і на основі загроз ІБ. У першому випадку периметри ІБ визначаються як умовні кордони, що розділяють зони з різними (необхідними) рівнями безпеки.

На практиці периметри утворюються шляхом виділення деяких функціональних областей ІС з ідентичними вимогами забезпечення ІБ. У другому випадку периметри утворюються на основі можливих загроз ІБ.

Для ЄІЦ пропонуються наступні периметри, рис. 4.

Стосовно до двох варіантів концептуального побудови ЄІЦ пропонується наступний розподіл сервісів ІБ по периметрах системи кіберзахисту, рис. 5, 6.

Для побудови ефективної системи захисту інформації (СЗІ), вибору і впровадженню адекватних технічних засобів повинен передувати опис, аналіз і моделювання загроз й уразливостей інформаційної системи та проведений на їх основі розрахунок й аналіз ризиків ІБ. Отже, очевидним є те, що спочатку кожна загроза повинна бути впізнана й ідентифікована.

Зазначимо, що використовувані в сучасних системах виявлення й протидії кібератакам, методи є досить ефективними в тому разі, якщо відомі точні характеристики нападу на інформацію або загрози ІБ.

Незалежно від використовуваних методів виявлення кібератак на ЄІЦ, ІС та АСК ТГ зустрічаються з однаковою проблемою – постійно змінювані характеристики нападів вимагають гнучкої СЗІ, яка здатна залишатися ефективною, навіть якщо не відомі точні характеристики нападу на інформацію, а також її ознаки [6, 7, 20, 21].


Рис. 4. Периметри забезпеченні ІБ ЄІЦ

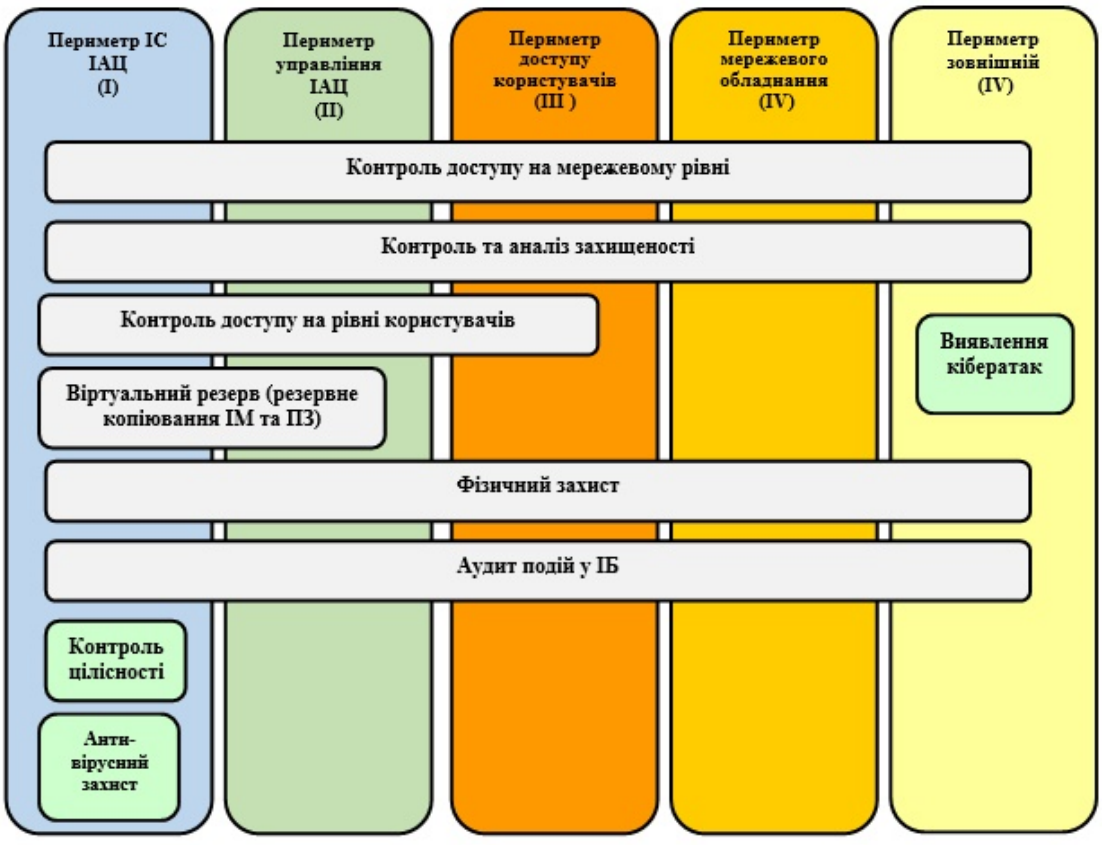


Рис. 5. Підсистеми ІБ для централізованого варіанта ЄІЦ

Неповнота інформації про загрози ІБ у ІКСТ є двоякою. По-перше, це часткова відсутність апріорної інформації, навіть на рівні уявлення про структуру всього об'єкта нападу на інформацію, що має, як правило, стохастичну природу. По-друге, обмежена можливість спостереження об'єкта нападу й розпізнавання загроз, що належать певному класу. У граничному випадку заздалегідь відома лише загальна множина загроз ІБ і способів їх реалізації.

Однак, як показує практика, одна з основних характеристик сучасних загроз полягає у тому, що вони довгий час не активуються, іноді до двох-трьох років [7, 8]. Цільові атаки, зокрема спрямовані на ІС підприємств, об'єкти інфраструктури, енергетики, транспорту тощо, зазвичай розробляються з урахуванням того середовища, на яке вони будуть націлені. Сучасні загрози створюються таким чином, щоб обійти захист, і, як правило, вже не виявляються за допомогою сигнатур. Розробка сценаріїв кібератак виконується з дотриманням всіх стандартів і технологій, з технічним завданням, робочим проектом, тестуванням, підтримкою і оновленням.

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

Вихідними даними для всіх КСТ є дані, що містяться у базі знань – REP:

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

де SYS – дані про інфраструктуру ІКСТ, яке підлягає захисту (топологія, склад елементів, користувачі, методи та засоби кіберзахисту та ін.); Events – дані про події кібербезпеки (КБ), які пройшли попередню обробку і знаходяться в базі знань на зберіганні; TAI – дані про сценарії кібератак у вигляді шаблонів [7, 20, 21]; NIS – дані про можливі контрзаходи протидії атакам і т. п.; gov – вирішальне правило на основі нечіткого регресійного механізму висновку про загрози кібератак в рамках політики безпеки (ПБ) ІКСТ.

Завдання, які вирішуються системою розпізнавання кібератак можуть бути записані таким чином:

Аналіз захищеності ІКСТ:

$$\mathrm{IOFP}_j = \mathrm{FS}(\mathrm{SYS}, \mathrm{TAI}, \mathrm{AT}, \mathrm{gov}), \quad (2)$$

де $\mathrm{IOFP}_j$ – значення j-го показника захищеності; AT – події, пов'язані із порушенням КБ, що відображають кібератаку; FS – функція, яка визначає $\mathrm{IOFP}_j$ на основі прийнятої ПБ.

Важливість подій пов'язаних із порушенням кібербезпеки можна визначити наступним чином.

Моделювання кібератак:

$$\mathrm{ESC}_{cr} = \mathrm{Model}(\mathrm{SYS}, \mathrm{TAI}, \mathrm{AT}, \mathrm{gov}, \mathrm{T}), \quad (3)$$

де $\mathrm{ESC}_{cr} \subset \mathrm{SYS}$ – критичний елемент ІКСТ; Model – модель кібератаки; T – проміжок часу, за який здійснюється кібератака.

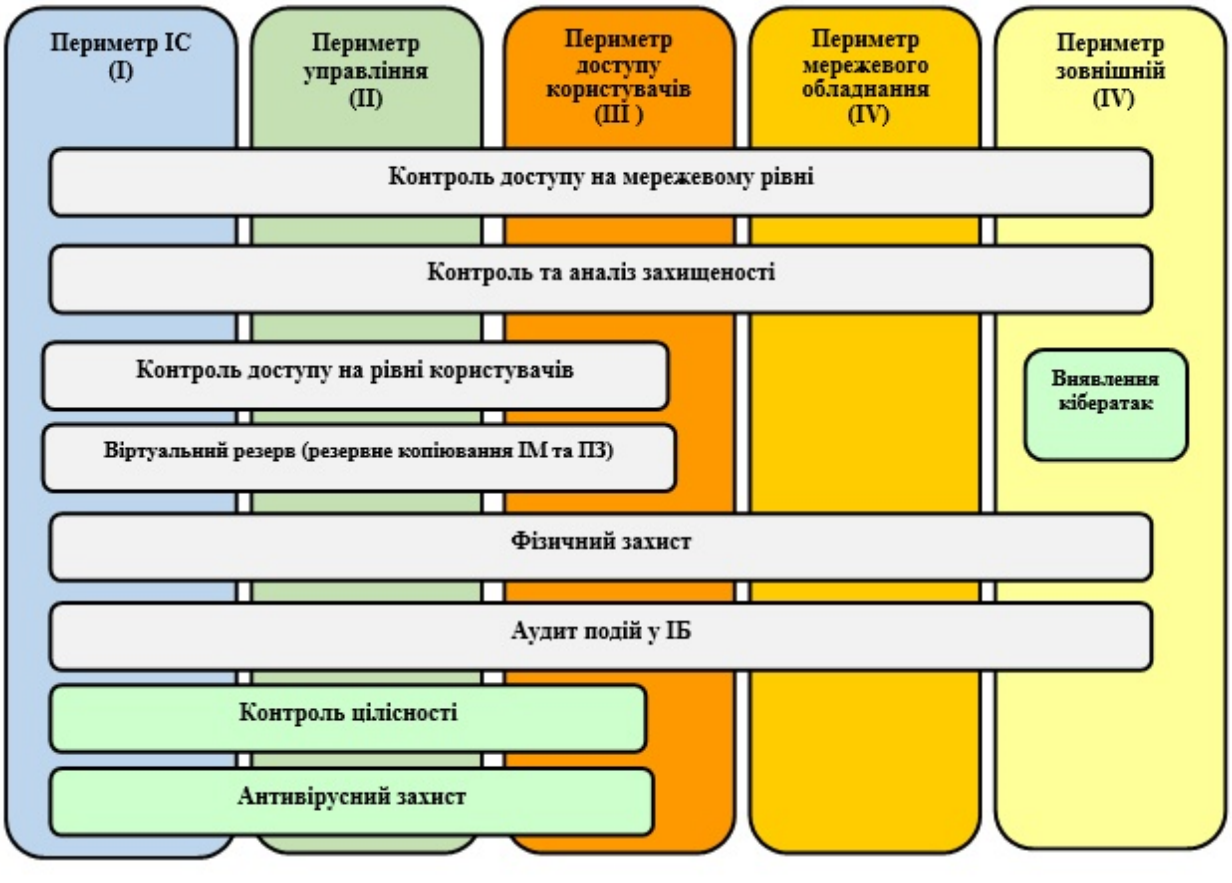


Рис. 6. Підсистеми ІБ для децентралізованого варіанта ЄІЦ

Підтримка прийняття рішень (або експертна система) для прийняття рішень для виявлення кібернападів на ІКСТ:

$$CM = \arg \min \left| IOFP - IOFP_{rt} \right|, \quad (4)$$

де $CM \subset gov$ – оптимальний контрзахід (система захисту інформації – СЗІ), що є елементом вирішального правила в рамках ПБ ІКСТ; IOFP та $IOFP_r$ – поточне та еталонне значення показника захищеності ІКСТ, відповідно.

Загроза зміни стану КБ ІКСТ представлена у наступному вигляді:

$$S_R = \left\langle EUM^*, SDN, RDN, ADN, MIF, IR \right\rangle, \quad (5)$$

де $EUM^*$ – множина сутностей, до складу якої входить: підмножина вузлів ІКСТ – $um^*$ (потенційні уразливості); SDN – множина суб'єктів ІКСТ; RDN – множина ребер графа станів системи (МРГСС) $S_R$, у тому числі тих, що відповідають правам доступу користувачів до $EUM^*$; ADN – МРГСС $S_R$, що відповідають отриманому доступу до $EUM^*$; MIF – МРГСС $S_R$, що відповідають інформаційним потокам між $EUM^*$ ($um^* \subset EUM^*$); IR – функція ієрархії $EUM^*$.

Введемо наступні позначення: MI – загальне число кіберзагроз для ІКСТ; $NP_{p_a}$ – деякий набір з $r_{p_a}$, $r_{p_a} \le MI$ різних цілочислених ознак кібернападів виду $\{p_{aj_1},...,p_{aj_r}\}$. Інтелектуальне розпізнавання загроз для кібербезпеки ІКСТ виглядає так.

1. У множині ознак кібернападів $\{p_{a_1},...,p_{a_{jMI}}\}$ виділяють сукупність різних підмножин виду

$$NP_{p_a} = \{p_{aj_1},...,p_{a_{MI}}\}.$$

2. Виділені підмножини називають опорними множинами розпізнавання кіберзагроз, а вся їхня сукупність позначається через $\Omega MI$.

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

4. Виконують процедуру обчислення оцінок. Розпізнаваний об'єкт кібератаки $sp_{an}$ порівнюють з кожним об'єктом який використовувався для навчання (ОВН) $sp_{ai}$ за кожною опорною множиною, наприклад, для кожного шаблону кібератаки.

5. Для кожного класу кіберзагроз для ІКСТ KL, $KL \in \{KL_1,...,KL_l\}$, обчислюють оцінку приналежності $\Gamma(sp_a, KL)$ об'єкта $sp_a$ до класу KL, яка має вигляд:

$$\Gamma(sp_a, KL) = \frac{1}{|LW_{KL}|} \sum_{sp_{ai} \in KL} \sum_{NP_{p_a} \in \Omega MI} po_{sp_a} \cdot po_{NP_{pa}} \cdot BN, \quad (6)$$

де $|LW_{KL}| = |KL \cap \{sp_{a1},...,sp_{aMI.}\}|$, BN – параметр який оцінює близькість об'єктів $sp'_a$ і $sp''_a$ з переліку РА – можливих цілей кібератак на ІКСТ за набором ознак $NP_{p_a}$. 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 така система лінійних нерівностей:

$$\Gamma(sp_{a1}, KL_1) > \Gamma(sp_{a1}, KL_2), \Gamma(sp_{aMI_1}, KL_1) >$$
$$> \Gamma(sp_{aMI_1}, KL_2), \Gamma(sp_{aMI_{1+1}}, KL_2) > \Gamma(sp_{aMI_{1+1}}, KL_1).$$
$$. \ . \ .$$
$$\Gamma(sp_{aMI}, KL_2) > \Gamma(sp_{aMI}, KL_1).$$

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, знаходять її максимальну спільну підсистему й з рішення цієї підсистеми визначають значення параметрів $po_{sp_{ai}}$ і $po_{NP_{pa}}$. 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 $po_{NP_{pa}}$.

Побудова множини елементарних класифікаторів для модельованого класу кібератак KL, $KL \in \{KL_1,...,KL_l\}$ зводиться до такого:

1) задають характеристичну функцію;

2) будують диз'юнктивна нормальна форма, що реалізує цю функцію;

3) обчислюють припустиму (максимальну) кон'юнкцію, що визначає приналежність об'єкта до певного класу кібератак на ІКСТ.

Метод та моделі інтелектуального розпізнавання загроз доповнено нечіткими множинами ознак нападу на інформацію. Для формалізації лінгвістичних змінних вибрано дзвіноподібну модель функції належності, яка має найменше число параметрів, що зменшує розмірність задачі підбору цих параметрів при навчанні [21].

Вирішальне правило gov(x), яке описує змін стану ІС або АСК в результаті кібератаки, можна представити в такому вигляді (табл. 1).

Таблиця 1

Вирішальне правило gov($p_{axi}$) для визначення стану ІКСТГ у випадку загрози для ІБ

| Правило | Вихідний стан, $S_R$ | Результуючий стан, ′ |
|---|---|---|
| $gov(p_{axi}) =$ $= (SDN_x,$ $SDN_y,$ $EUM^*_z,$ $eum_l,$ $pro^m_r)$ | $SDN_x, SDN_y, pro^m_r \in EUM^*, eum_l,$ $EUM^*_z \in EUM, eum_l \in pro^m_r,$ $(SDN_x, eum_l, write_r / read_r \in RDN),$ $EUM^*_z \in SDN_y$ або $SDN_x = SDN_y,$ або $(EUM^*_z, SDN_x, write_m / read_m)$ $\in MIF, KL, MC \in AL(KL)$ | $S_R = S'_R$, $EUM^* = EUM'^*,$ $ADN = ADN', IR = IR',$ $MIF = MIF', RDN' = RDN'(SDN_x,$ $SDN_y), KL \in (KL_1,...KL_l),$ $MC \in AL$ $(KL \in (KL_1,...KL_l))$ |

Таким чином, вирішальне правило gov формулюється на основі нечіткого регресійного механізму висновку про загрози кібератак на базі розробленого методу інтелектуального розпізнавання загроз, суть якого полягає у визначенні кон'юнкцій за покриттям класів кіберзагроз ІБ ІКСТ. Метод відрізняється від існуючих застосуванням дискретних процедур із використанням апарату логічних функцій та нечітких

множин ознак нападу на інформацію, що дозволяє створювати ефективні аналітичні, схемотехнічні та програмні рішення для систем захисту ІКСТ.

Для кожного класу загроз складалася навчальна вибірка з 100–200 об'єктів ($sp_{an}$), розбитих на відповідні класи кіберзагроз для ІКСТ [21]. Для кожного класу кількість ознак кібератак варіювалася від 3 до 9. Інформативність ознаки змінювалася в діапазоні від –1 до +1. Для оцінки ефективності процедур розпізнавання використовувався метод ковзного контролю.

Ймовірність розпізнавання кібератак $P_{рз}$ для ІКСТ обчислюється за виразом

$$P_{рз} = \Phi\left(\frac{0{,}5\cdot\sum_{i=1}^{N_{pa}}\left[1+\Phi(IZ_{p_{axj}}/2)\cdot\log_2 n_i\right]}{2\cdot N_{pa}}\right), \qquad (7)$$

де $\Phi$ – інтеграл ймовірності; $N_{pa}$ – кількість ознак кібератаки на компоненти ІКСТ; $n_i$ – число градацій ознаки нападу на інформацію.

Приклади результатів тестування процедурі розпізнавання кібератак показані на рис. 7.

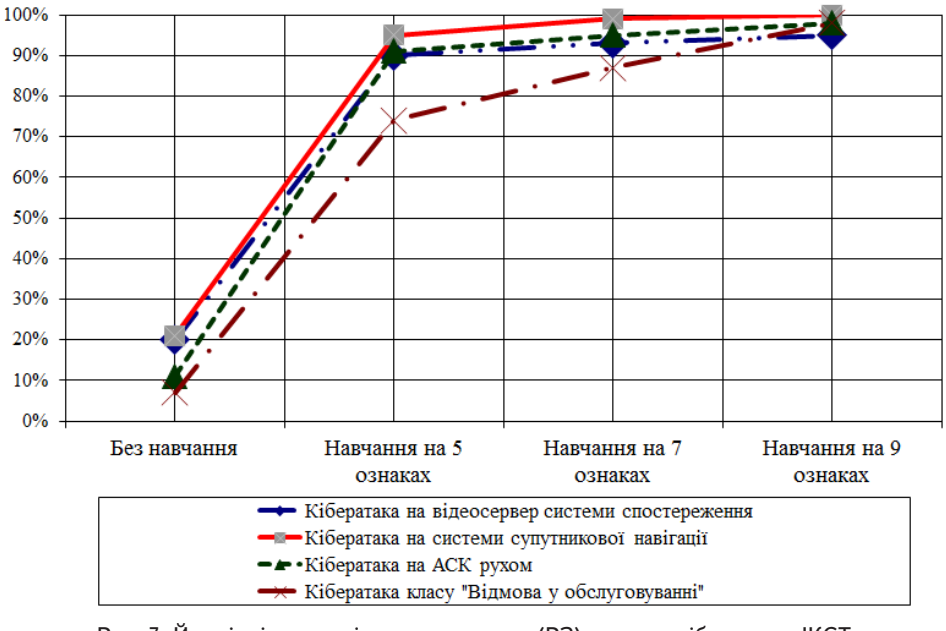


Рис. 7. Ймовірність розпізнавання загроз (РЗ) типових кібератак у ІКСТ

## 6. Обговорення результатів дослідження

Таким чином, описані моделі розпізнавання кіберзагроз для ІКСТ не тільки становлять самостійний практичний інтерес, але і є прикладом можливої формалізації опису нових, ще невідомих класів кібератак. Певна громіздкість необхідних розрахунків дещо ускладнює практичне застосування запропонованої моделі, але, в експонентному наближенні розрахунки ймовірності реалізації кібернападів на ІС та АСК ТГ виявляються досить простими. Наведений метод розпізнавання загроз дозволяє перейти до кількісних процедур оцінки можливостей реалізації кібернападів у ІКСТ й тим самим підвищити обґрунтованість проведених заходів із захисту інформації.

Перспективи подальших досліджень полягають у тому, щоб визначити найбільш критичні об'єкти ІКСТ, що підлягають захисту, а також дослідити запропонований метод інтелектуального розпізнавання загроз на більш широкому класі задач кількісного і якісного розпізнавання кібернападів.

## 7. Висновки

1. Розглянуті питання впровадження сучасних інформаційно-комунікаційних систем і технологій у транспортній галузі України. Проаналізовано сучасний стан кіберзахисту ТГ України. З'ясовано, що складність застосування до систем розпізнавання загроз формалізованого апарату аналізу й синтезу систем кіберзахисту ІКСТ полягає в тому, що конкретний інформаційний комплекс і його підсистема ІБ складаються з різнорідних елементів, які описуються із використанням різних математичних моделей. Розглянута можливість створення захищеного ІКСТ, адаптованого до умов формування єдиного інформаційно-комунікаційного простору транспортної галузі, за умов збільшення кількості дестабілізуючих впливів на кібербезпеку ІС та АСК транспорту.

2. Розроблено метод інтелектуального розпізнавання загроз на основі дискретних процедур із використанням апарату логічних функцій та нечітких множин, що дозволяє підвищити ефективність розпізнавання загроз ІКСТ, створювати ефективні аналітичні, схемотехнічні та програмні рішення СЗІ ІКСТГ.

Література

1. U.S. Department of Transportation, Research and Innovative Technology Administration, "Intelligent Transportation Systems (ITS) Strategic Plan: Background and Processes [Electronic resource]. – 2010. – Available at: http://www.its.dot.gov/strategic_plan2010_2014/ppt/strategic_backgroundv2.ppt
2. Sadek, A. W. Special Issue on Cyber Transportation Systems and Connected Vehicle Research [Text] / A. W. Sadek, B. "Brian" Park, M. Cetin, // Journal of Intelligent Transportation Systems: Technology, Planning, and Operations. – 2014. – Vol. 20, Issue 1. – P. 1–3. doi: 10.1080/15472450.2014.889914

3. Transportation & Logistics 2030 [Text]. – Vol. 4: Securing the supply. – P. 254–286.
4. Дудикевич, В. Б. Проблеми оцінки ефективності систем захисту [Текст] / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету «Львівська політехніка». Сер.: Автоматика, вимірювання та керування. – 2012. – № 741. – С. 118–122.
5. Корченко, А. А. Система формирования нечетких эталонов сетевых параметров [Текст] / А. А. Корченко // Захист інформації. – 2013. – Т. 15, № 3. – С. 240–246.
6. Sommestad, T. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour [Text] / T. Sommestad, H. Karlzén, J. Hallberg // International Journal of Information Security and Privacy. – 2015. – Vol. 9, Issue 1. – P. 26–46. doi: 10.4018/ijisp.2015010102
7. Грищук, Р. В. Атаки на інформацію в інформаційно-комунікаційних системах [Текст] / Р. В. Грищук // Сучасна спеціальна техніка – 2011. – № 1 (24). – С. 61–66.
8. Yakovyna, V. Software Reliability Assessment Using High-Order Markov Chains, [Text] / V. Yakovyna, D. Fedasyuk, O. Nytrebych, I. Parfenyuk, V. Matselyukh // International Journal of Engineering Science Invention. – 2014. – Vol. 3, Issue 7. – P. 1–6.
9. Car hacking: The security threat facing our vehicles [Text]. – Popular Science, 2014. – P. 67–73.
10. Харченко, В. П. Кибертерроризм на авиационном транспорте [Текст]: зб. наук. пр. / В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк // Проблеми інформатизації та управління. – 2009. – Вип. 4 (28). –С. 131–140.
11. Вильский, Г. Б. Информационные риски судовождения [Текст] / Г. Б. Вильский // Наук. Вістник ХДМА. – 2012. – № 1(4). – С. 17–26.
12. Мірошник, М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах [Текст] / М. А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2015. – № 4 (113). – С. 39–43.
13. Крылова, В. А. Разработка методов оценки эффективности систем защиты информации в распределенных компьютерных системах [Текст] / В. А. Крылова, А. Н. Мирошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2015. – № 2 (111). – С. 43–51.
14. 2015 Cyber Attacks Statistics [Electronic resource]. – 2016. – Available at: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/
15. Основная статистика за 2015 год [Электронный ресурс]. – 2016. – Режим доступа: https://securelist.ru/files/2015/12/KSB_2015_Stats_FINAL_RU.pdf
16. MITRE Research Program [Electronic resource]. – Available at: http://www.mitre.org
17. Walk, T. Cyber-attack protection for pipeline SCADA systems [Text] / T. Walk. – Pipelines International digest, 2012. – P. 5–8.
18. Maras, M-H. Cybercrime Laws: Which Statute for Which Crimes [Text] / M-H. Maras. – Computer Forensics: Cybercriminals, Laws, and Evidence. Sudbury, MA: Jones & Bartlett Learning, 2012. – P. 104–106.
19. Creating trust in the digital world EY's Global Information Security Survey 2015 [Electronic resource]. – Available at: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf
20. Корченко, О. Г. Ознаковий принцип формування класифікацій кібератак [Текст] / О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк, В. М. Кінзерявий, С. В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2010. – № 1. – С. 32–38.
21. Lahno, V. Ensuring of information processes' reliability and security in critical application data processing systems [Text] / V. Lahno // MEST Journal. – Belgrade. – 2014. –Vol. 2, Issue 1. – P. 71–79. doi: 10.12709/mest.02.02.01.07