© Lakhno V. Increase the cybersecurity of transport information and communications systems // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 44-50.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТРАНСПОРТУ

Валерій Лахно

Європейський університет, Україна

ЛАХНО Валерій Анатолійович, д.т.н.

Рік та місце народження: 1964 рік, м. Луганськ, Україна.
Освіта: Луганський машинобудівний інститут (з 2001 року Східноукраїнський Національний університет імені Володимира Даля), 1987 рік.
Посада: завідувач кафедри організації комплексного захисту інформації.
Наукові інтереси: інформаційна безпека, безпека інформаційно-комунікаційних систем.
Публікації: більше 100 наукових публікацій, серед яких монографії, навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: valss21@ukr.net

Анотація. *Інформаційно-комунікаційне середовище транспорту (ІКСТ) орієнтоване на взаємодію з іншими секторами економіки для скорочення затримок при транспортуванні вантажів, обробці морських і річкових суден, контейнерів, залізничних вагонів і вантажів на прикордонних переходах на основі використання систем електронних накладних, системи «клієнт-банк», e-business, взаємодії із клієнтурою й партнерами тощо. Критичність виходу з ладу систем такого рівня складності вимагає нових досліджень питань забезпечення інформаційної безпеки (ІБ) ІКСТ з акцентом на доступність та стійкість систем, а також цілісності інформації, яка зберігається та опрацьовується в інформаційних системах (ІС) та автоматизованих системах керування (АСК) галузі. Стаття містить результати досліджень, які спрямовані на подальший розвиток методів та моделей розпізнавання загроз ІКСТ та удосконалення ІБ в умовах формування єдиного інформаційно-комунікаційного середовища, впровадження нових та модернізації існуючих ІС на транспорті, і збільшення кількості дестабілізуючих впливів на доступність, схоронність і цілісність інформації. Запропоновано метод розпізнавання загроз на основі дискретних процедур з використанням апарату логічних функцій та нечітких множин, що дозволяє підвищити ефективність розпізнавання, створювати ефективні аналітичні, схемотехнічні та програмні рішення для систем захисту інформаційних ресурсів ІКСТ.*

Ключові слова: *інформаційно-комунікаційне середовище транспорту, захист інформації, інформаційна безпека, розпізнавання загроз, дискретні процедури.*

Вступ

Активне розширення інформаційно-комунікаційного середовища транспорту (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 ІБ та захистом інформації, а також виявлених уразливостей у інформаційних системах (ІС) та автоматизованих системах керування (АСК). Загрози є цілком реальними, оскільки злочинці можуть отримати можливість перехоплювати паролі, окремі файли, геолокаційну інформацію, транслювати аудіо- та відеодані, контролювати Wi-Fi-мережі, веб-камери, інформаційні табло на автомобільних і залізничних шляхах, вокзалах, аеропортах та ін. [1-6].

Враховуючи вище зазначене, варто зупинитися на таких передумові захисту ІКСТ, як невід'ємна складова національної безпеки.

По-перше, важливість транспортної галузі (ТГ) в національній безпеці та економіці окремих держав.

По-друге, необхідність гарантувати безпеку транспортного процесу та його інформаційної складової, роль якої постійно зростає.

По-третє, з інтеграцією держав східної Європи до євразійських транзитних коридорів, інформаційні ресурси набувають для галузі такого ж

значення, як матеріальні й виробничі.

По-четверте, значна уразливість ІС та АСК ТГ, що пов'язано з появою нових методів нападів на інформацію, зокрема комп'ютерних (КНІ), значним поширенням бездротових комунікацій, систем навігації із використанням GPS, ГЛОНАСС, GALILEO, систем відеоспостереження (SC), технологій зв'язку GSM-R, VSAT, систем диспетчерського управління (SCADA, HMI), PLC на різних видах транспорту та ін.

По-п'яте, необхідність розроблення принципів побудови захищеного ІКСТ і методики управління інформаційно-обчислювальним процесом, на підставі комплексного застосування існуючих засобів і методів захисту та зберігання інформації в інтересах підтримки стійкої працездатності ІС та АСК транспорту.

Аналіз існуючих досліджень

Об'єктом нападу на інформацію може стати будь-який з елементів ІКСТГ. Проте в цілому всі елементи ІКСТГ можуть бути віднесені до однієї з наступних категорій: центри опрацювання даних (ЦОД), АСК, ІС системи SCADA, HMI; периферійне обладнання та PLC; системи та канали зв'язку для обміну даними. Для ІС та АСК транспорту характерними є наступні види (табл. 1): бортові засоби, що встановлюються на рухомі об'єкти ІКСТ (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; ситуаційні, диспетчерські та оперативні центри; засоби забезпечення зв'язку - Інтернет, мережа GSM/GPRS, GSM-R, VSAT, супутниковий зв'язок; інформаційно-телекомунікаційні засоби, що забезпечують захищену інформаційну взаємодію із зовнішніми інформаційними системами [3, 4, 5, 7, 8, 11, 12].

Таблиця 1

Цілі, об'єкти та суб'єкти нападу на інформацію у ІКСТГ

<table>
<tr><td colspan="7">Цілями нападу на ІКСТГ можуть бути</td></tr>
<tr><td>Кібершпіонаж - несанкціонована передача за допомогою прихованих (незадекларованих) каналів зв'язку даних, програм АІС, ІС, АСК ТГ або географічних координат (GPS або ГЛОНАС та ін. технології).</td><td>Кібераудит - розробка сценаріїв КНІ, хакерські і «дружні» кібератаки, пошук уразливостей ІКСТГ.</td><td colspan="2">Кібершахрайство - «продаж» фальшивих електронних квитків, злом автоматів продажу квитків і квитанцій оплати багажу, злом лічильників обліку вантажів, енергоносіїв і автоматичних витратомірів і заправників та ін.</td><td>Кіберсаботаж - зниження пропускної здатності автомобільних, залізничних, трубопровідних магістралей, зокрема, до повної зупинки транспортних процесів.</td><td colspan="2">Кібердиверсії - створення ворожих (помилкових) і небезпечних маршрутів прямування (руху), особливо при перевезенні особливо небезпечних і соціально-значущих вантажів, пасажирських та військових перевезеннях.</td></tr>
<tr><td colspan="7">Види транспорту та об'єкти нападу</td></tr>
<tr><td>Залізничний  </td><td>Авто-мобільний  </td><td>Повітряний  </td><td>Морський та річковий  </td><td>Трубо-провідний  </td><td>Муніци-пальний  </td><td>Системи навігації  </td></tr>
<tr><td colspan="7">Об'єктами кібератак можуть бути системи диспетчерського та автоматизованого управління (АІС, ІС, АСК, SCADA, PLS, HDI), відповідальні за формування безпечних маршрутів руху рухомого складу (РС), системи безпечного руху РС і безпечного проїзду переїздів для з/т, системи захисту і регулювання електропостачання, автоматичні системи пожежогасіння та термостабілізації, системи автоматики у морських та річкових портах, залізничних депо, АТП та ін., системи зв'язку GSM-R, VSAT та ін., а також оператори, обслуговуючий персонал – диспетчери, чергові, і машиністи з/т, водій АТ, екіпажі суден та повітряного транспорту.</td></tr>
<tr><td colspan="7">Атакуюча сторона</td></tr>
<tr><td colspan="7">Хакери, конкуренти, інсайдери, організовані злочинні угруповання, спецслужби, збройні сили іноземних держав (кібервійска). При цьому рівень «озброєності» (технічної оснащеності) і компетентності (інформаційної обізнаності) «зловмисника» може бути дуже високим.</td></tr>
</table>

До складу технологічного комплексу ІС та АСК ТГ можуть входити різноманітні технічні системи та засоби: системи і засоби координатно-часового, метеорологічного і т. п. видів забезпечення; системи, засоби, лінії та мережі зв'язку і передачі даних; системи і засоби дистанційного моніторингу; системи і засоби збору, накопичення та обробки інформації; автоматизовані системи і засоби управління; системи і засоби відображення і доведення інформації; інші технічні та програмно-технічні засоби.

Велика частина систем і засобів використовується для формування каналу зворотного зв'язку як з людиною-оператором, так і з

керованими технічними компонентами транспортної системи.

Практично кожна інформаційна або інформаційно-керуюча система, у тому числі на транспорті, може виступати об'єктом НСД, тобто сукупності дій зловмисника, спрямованих на порушення однієї із трьох властивостей інформації – конфіденційності, цілісності або доступності.

Дослідженням ІБ транспорту присвячено роботи: В.П. Бабака, Д.С. Бірюкова, В.С. Блінцова, Г.Б. Вільського, С.О. Гнатюка, О.О. Корнієнко, О.Г. Корченка, О.І. Стасюка, В.П. Харченка та ін. Однак в Україні ці дослідження носять фрагментарний характер [3, 8, 9, 10]. Моделі та алгоритми розпізнавання кібернападів часто не взаємопов'язані [3, 9], що наразі ускладнює їх використання при створенні ефективних інтелектуальних систем розпізнавання загроз та кібератак.

У разі можливого деструктивного впливу на критично важливі об'єкти інформатизації на транспорті з боку вороже налаштованих держав, терористичних або злочинних організацій в умовах гібридної війни проти України, рівень кіберзагроз для ІКСТ стрімко зростає. Досягнутий рівень інформатизації транспортної галузі (ТГ) без належного забезпечення кібербезпеки та захисту інформації вже несе в собі потенційні загрози. Нескладно собі уявити результати DoS/DDoS-атаки на інформаційну мережу Укрзалізниці, Автолюкс або МАУ. Результатом буде транспортний колапс у масштабах всієї держави. Навіть найменший збій в системах реалізації квитків на будь-який вид транспорту, або планування перевезень може викликати великі проблеми у функціонуванні ТГ.

Отже, потрібні подальші дослідження, спрямовані на розвиток методологічних та теоретичних засад захисту інформаційно-комунікаційного середовища транспорту як невід'ємної складової критично важливих комп'ютерних систем.

Метою даної роботи є побудова нових моделей та методів захисту інформаційно-комунікаційного середовища транспорту на основі розпізнавання кіберзагроз, що дозволить створювати адаптивні інтелектуальні системи захисту інформації за постійного збільшення кількості та складності кібератак.

Основна частина дослідження

Інформаційна безпека ТГ ніколи не виділялася в якості самостійного виду національної безпеки. Більше того, 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. При чому ІБ на транспорті об'єктивно має свої особливості і специфіку, що відображає галузеву спрямованість і визначальне її місце, роль і значення в структурі національної безпеки.

У зв'язку з цим, враховуючи безперервно зростаючу роль транспортної інфраструктури, слід виділити ІБ ТГ в якості важливого самостійного виду національної безпеки, див. рис. 1.

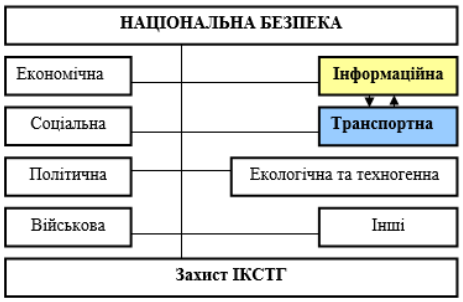

Рис. 1. Місце ІБ ТГ в загальній системі національної безпеки

Важливе значення має класифікація видів ІБ ТГ, що дозволяє здійснювати вибір конкретної політики та стратегії її забезпечення. В якості вихідних даних для класифікації доцільно виділити види транспортних підсистем як об'єктів ІБ, з урахуванням специфіки загроз для різних видів транспорту. В результаті вийде структура ІБ ТГ, яка представлена на рис. 2.

Рис. 2. Структура інформаційної безпеки на транспорті

Практика свідчить, що всі ці підсистеми ІБ тісно пов'язані між собою і знаходяться в діалектичній взаємодії. Крім того, слід чітко відрізняти «систему інформаційної безпеки на транспорті» від «системи забезпечення транспортної безпеки» як реальної системи структур, сил або коштів, які безпосередньо займаються діяльністю по забезпеченню транспортної безпеки. Це принципово різні поняття, що мають різні предметні області пізнання і практичної діяльності, де потрібна підготовка певних фахівців, відповідальних за забезпечення транспортної безпеки в цілому і окремих її видів.

Неповнота інформації про загрози ІБ у ІС та АСК ТГ 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, див. рис. 3.

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, 11]. 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 КНІ виконується з дотриманням всіх стандартів і технологій, з технічним завданням, робочим проектом, тестуванням, підтримкою і оновленням.

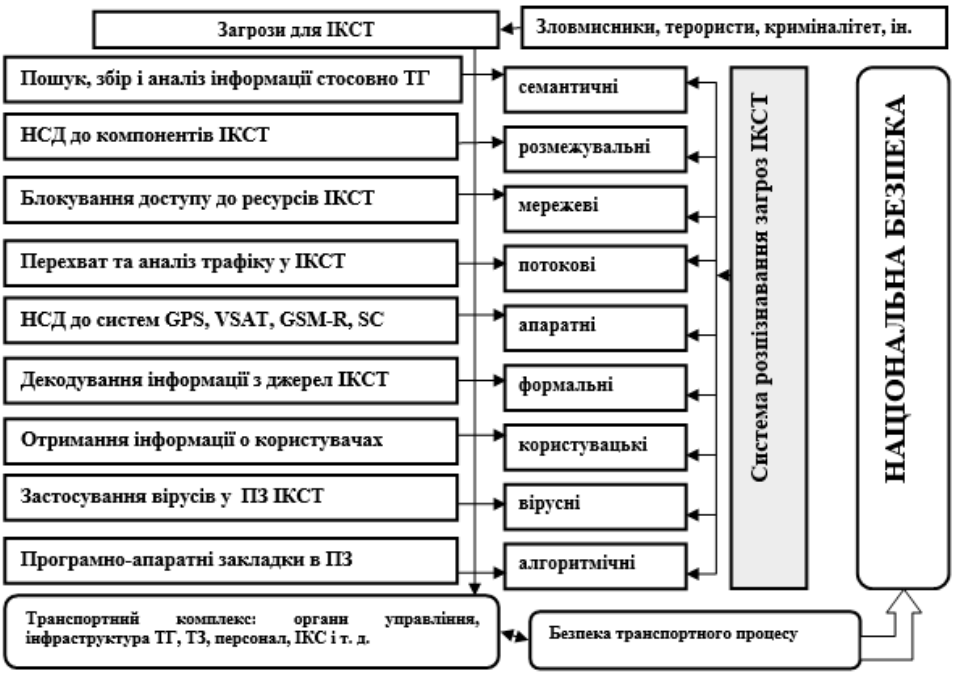

Рис. 3. Загрози для ІКСТ

На думку багатьох фахівців [3, 10, 12], перспективним шляхом підвищення функціональної ефективності систем розпізнавання кіберзагроз (СРКЗ) є впровадження інтелектуальних інформаційних технологій, основаних на методах та моделях машинного навчання. Математичний опис СРКЗ виглядає наступним чином:

$$\Delta = \left\langle G \times T \times PA \times \Phi \times R, Z^{|2|}, X^{|2|}, B_1, B_2 \right\rangle, \qquad (1)$$

де G – множина вхідних факторів (сигналів), які впливають на ІБ ІКСТ; T – множина моментів часу зняття інформації про стан ІБ (кіберзахищеності ІКСТ); PA – простір ознак для розпізнавання кіберзагроз ІКСТ; Φ – простір можливих функціональних станів ІБ ІКСТ; R – база знань для ідентифікації аномалій, кіберзагроз або кібератак; $Z^{|2|}$ – навчальна матриця (еталон) для двох класів; $X^{|2|}$ – бінарна навчальна матриця; B_1, B_2 – оператори формування вхідної та бінарної навчальних матриць, відповідно. Категорійна модель адаптивної системи інтелектуального розпізнавання загроз наведена на рис. 4.

Оператор $\Theta : X^{|2|} \to \Re^{|2|}$ використовується для розбиття простору ознак аномалій, кіберзагроз або кібератак на два класи розпізнавання. За допомогою параметра класифікації ψ перевіряється статистична гіпотеза про належність реалізацій до модельованого класу аномалій, кіберзагроз або кібератак.

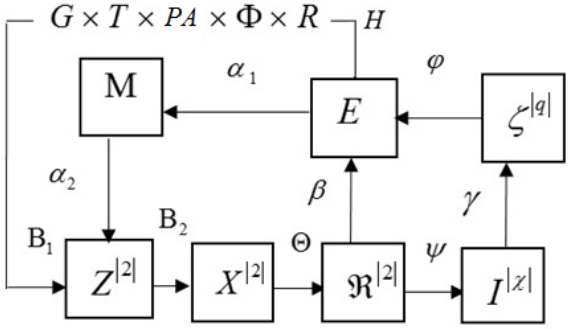

Рис. 4. Категорійна модель СРКЗ для ІКСТ

Шляхом оцінки статистичних гіпотез, за допомогою оператора γ, формується множина $\zeta^{|q|}$ яка характеризує точність розпізнавання СРКЗ, відповідно, χ – кількість статистичних гіпотез, $q = \chi^2$ – кількість характеристик СРКЗ. Оператор φ формує множину E, яка складається із значень інформаційного критерію функціональної ефективності СЗКЗ. Оператор β використовується для оптимізації системи контрольних відхилень СРКЗ. Множина M, замикається послідовно оператором $\alpha_1 : E \to \mathrm{M}$ і оператором $\alpha_2 : \mathrm{M} \to Z$,

який змінює реалізації ознак аномалій, кіберзагроз або кібератак в процесі навчання СРКЗ.

При побудові дискретних процедур розпізнавання загроз (ДПРЗ) ІБ ІКСТ введено поняття елементарного класифікатора, під яким розуміють фрагмент опису ОВН. Для кожного класу загроз ІБ будують множину елементарних класифікаторів із заздалегідь заданими властивостями. Запропоновано метод побудови розв'язувального (вирішального) правила $\text{gov}(\text{p}_{\text{axi}})$ для інтелектуального розпізнавання загроз ІКСТ, при якому розпізнавання проводилося б з мінімальною кількістю помилок.

Загрозу зміни стану ІБ ІКСТГ представлено у такому вигляді:

$$S_R = \left\langle EUM^*, SDN, RDN, ADN, MIF, IR \right\rangle, \qquad (2)$$

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

Головною особливістю запропонованого методу інтелектуального розпізнавання загроз ІКСТ є можливість одержання результату за відсутності інформації про функції розподілу значень ознак і за наявності малих навчальних вибірок. Основне завданням побудови ДПРЗ – пошук інформативних підописів (або фрагментів описів).

Інформативними вважаються фрагменти, які відображають певні закономірності в описах об'єктів, використовуваних для навчання. У ДПРЗ для 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 ІКСТ.

Як інформативну значущість ознаки атаки на ІКСТ p_{axj} будемо розглядати величину:

$$\text{IZ}_{\text{p}_{\text{axj}}} = \frac{\sum\limits_{(sp'_a, NP_{pa}) \in \text{MC}^{\text{AL}}(KL),\ p_{axj} \in NP_{pa}} \text{vop}_{(sp'_a, NP_{pa})}}{\sum\limits_{(sp'_a, NP_{pa}) \in \text{MC}^{\text{AL}}(KL)} \text{vop}_{(sp'_a, NP_{pa})}}, \qquad (3)$$

де $\text{vop}_{(sp'_a, NP_{pa})}$ – функція значності елементарного класифікатора (ЕК) загрози для ІБ ІКСТ; MC - множина усіх ЕК, породжених наборами ознак загрози нападу на ІС або АСК $\{p_{ax1}, ..., p_{axn}\}$; $\text{NP}_{\text{p}_\text{a}}$ - базовий набір ознак класу KL нападу на ІС або АСК ($\text{NP}_{\text{p}_\text{a}} = \{p_{ax_{j1}}, ..., p_{ax_{jr}}\}$); KL – класи загроз для ІБ ІС та АСК ІКСТ; AL – множина алгоритмів розпізнавання загроз.

Побудова множини елементарних класифікаторів для модельованого класу загроз 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 ІБ ІКСТ.

Для кожного із співвідношень дерева висновку побудовані нечіткі бази знань, які представляють сукупність нечітких правил «якщо-тоді», що визначають взаємозв'язок між вхідними та вихідною змінними при оцінці ІБ КІС. За нечіткими базами знань складені логічні рівняння. Правило активується, якщо істинність його умови більша за нуль.

Для оцінки ефективності процедур розпізнавання використовувався метод ковзного контролю. Ймовірність розпізнавання загрози $P_{рз}$ для ІБ ІКСТ обчислюється за виразом:

$$P_{рз} = \Omega\left(\frac{0{,}5 \cdot \sum\limits_{i=1}^{N_{pa}} \left[1 + \Omega(\text{IZ}_{\text{p}_{\text{axj}}} / 2) \cdot \log_2 n_i\right]}{2 \cdot N_{pa}}\right), \qquad (4)$$

де Ω – інтеграл ймовірності; N_{pa} – кількість ознак нападу на інформацію; $\text{IZ}_{\text{p}_{\text{axj}}}$ – інформативність значення ознаки атаки; n_i – число градацій ознаки нападу на інформацію.

Метод складання вирішального правила $gov(p_{axi})$ для визначення стану S_R систем у випадку загрози для ІБ, базують на процедурі аналізу критичності окремих елементів ІКСТ і визначають етапами:

1) для кожного вузла $um^* \subset EUM^*$ визначають довірених користувачів, що володіють правом доступу до кожної сутності (наприклад, інформаційного масиву – $M_{k\,\text{inf}}$);

2) множини EUM^*, SDN й функцію IR не змінюють на всіх траєкторіях графа станів системи;

3) для одержання зловмисником (суб'єктом-порушником) SDN_x права володіння щодо суб'єкта SDN_i йому, як правило, потрібно одержати доступ не тільки до сутності EUM_z^*, але й доступ на запис/читання до деякої сутності $\text{eum}_\text{l} \in \text{EUM}^*$, що є інтерфейсом або портом деякого суб'єкта-процесу $pro \in SDN$, що здійснює надання прав доступу SDN_i на основі даних у сутності EUM^*;

4) сутності EUM_z^* і eum_l є асоційованими із суб'єктом pro_r^m; сутності eum_l й pro_r^m, як правило, розміщені на одному вузлі мережі, а сутності EUM_z^* й EUM_y^* можуть бути розміщені на різних вузлах ІКСТГ;

5) вирішальне (розв'язувальне) правило $gov(x)$, яке описує стани ДЄІІС, ІСТГ або АСК, можна представити в такому вигляді (див. табл. 2).

Вирішальне правило $\text{gov}(p_{axi})$ для визначення стану ІКСТ у випадку загрози для ІБ Таблиця 2

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

Результати дослідження

Приклади результатів тестування ДПРЗ для ІБ ІКСТ показані на рис. 5. Під час виконання тестових завдань з розпізнавання загроз (РЗ) НСД до програмного забезпечення та баз даних (ПЗ та БД) ІКСТ, систем супутникової навігації та систем керування рухом на наземному транспорті, ймовірність розпізнавання загроз ІКСТ залежно від класу атак склала 85–98 %.

Аналіз рис. 5 показує, що досить ефективним в алгоритмі розпізнавання загроз є використання 3-4 ознак, що свідчить про побудову безпомилкових вирішальних правил для ДПРЗ.

Під час тестів використовували представницькі набори обмеженої довжини. Максимальну довжину набору ознак класу нападу на інформаційні ресурси ІС або АСК брали рівною 3. При меншій максимальній довжині більша частина об'єктів не містила жодного представницького набору. А збільшення максимальної довжини до 4 значно збільшує час роботи алгоритму.

У завданні розпізнавання нападу на інформацію в ІКСТ частина значень ознак має вагу, близьку до нуля, але при цьому багато і таких значень, які мають досить велику вагу, тобто є дуже типовими для одного із класів.

Якщо розташувати ознаки класу нападу на ІС або АСК в порядку зниження інформативності, то, як правило, у кожному класі виділено групу ознак з великою інформативністю, далі йде деякий розрив, а ознаки, що потім залишилися, вибудовують в ряд із плавно зменшуваною інформативністю.

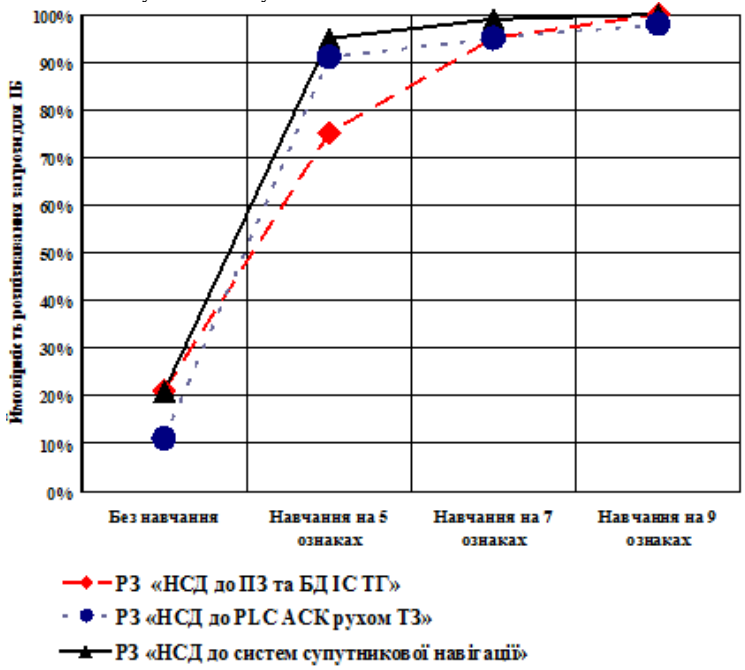

Рис. 5. Ймовірність розпізнавання загроз (РЗ) типових нападів на інформацію у ІКСТ

Наприклад, у завданні оцінки впливу кібернападів на компоненти ІКСТ, зокрема, АСК рухом, як інформаційні ознаки можна використовувати: 1) зниження пропускної здатності каналу; 2) зміна частотної характеристики та ін.

У завдання оцінки впливу атаки на системи супутникової навігації, найбільш інформативними є наступні ознаки: 1) Рівень сигналу (Сигнал супутників GPS на поверхні Землі досить слабкий, його рівень – близько -163 дБ*Вт Сигнал, що випромінюється імітатором значно сильніше, що може свідчити про атаку); 2) Однаковий рівень сигналу від різних супутників (GPS-сигнали різних супутників зазвичай сильно відрізняються за рівнем); 3) Шум (Підроблений сигнал GPS має дуже низький рівень шуму); 4) Номери супутників та ін.

У результаті досліджень, також доведено, що інформативність набору значень ознак може суттєво (іноді на порядок) перевищувати вагу ознак, які його становлять. Інакше кажучи, фрагмент, породжений двома ознаками загроз, може більш сильно

характеризувати один із класів кібернападів, ніж значення кожної із зазначених ознак окремо.

Висновки

Основні результати досліджень полягають у такому: 1) проаналізовано сучасний стан захисту інформації та кібербезпеки ТГ України, доведено, що практично всі компоненти ІКСТ можуть стати об'єктом кібернападу; 2) розроблена категорійна модель, яка дозволяє на етапі аналізу системи розпізнавання кіберзагроз для ІКСТ, встановлювати відношення між елементами адаптивних систем кіберзахисту; 3) запропоновано новий метод розпізнавання загроз на основі дискретних процедур із використанням апарату логічних функцій та нечітких множин ознак кібернападів, що дозволяє підвищити ефективність розпізнавання загроз ІКСТ залежно від класу кібернападів до 85–98 %; 4) запропоновано метод формування вирішального правила для системи розпізнавання кіберзагроз на основі використовування ДПРЗ, який базується на процедурі аналізу критичності окремих елементів ІКСТ.

Література

[1] The role of IT in logistics / David J. Closs, Jim Davidson, Richard L. Dawe et al // The Official Magazine of the Logistics Institute. — 2007. —V. 27. — № 6.

[2] Transportation & Logistics 2030. Volume 4: Securing the supply. — P. 254-286.

[3] Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks. / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. — 2010. — Vol. 14, No 2. — p. 58-69.

[4] Talk at DEFCON 18, 2010 — James Arlen — SCADA and ICS (Online): http://youtu.be/AoOuHXnlfbc.

[5] Recommendations for the Improvement of Security in Public Transport Public Summary Only Reference SCR-WP11-D-UIP-041-PS (Online): http://www.secur- ed.eu/?p=1963.

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

[7] Copper Theft Threatens U.S. Critical Infrastructure, FBI Reports and Publications, September 14, 2008 (Online): — http://www.fbi.gov/news/stories/2008/december/copper-theft-intelreport-unclass.

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

[9] Вильский Г.Б. Информационная безопасность судовождения: монография / Г.Б. Вильский; Одес. нац. мор. акад. — Одесса, 2014. — 334 с.

[10] Lahno V. Protection of information in critical application data processing systems. / V. Lahno // MEST Journal. — Belgrade. — 2014. — Vol. 2, No 2. — P. 102-112.

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

[12] Alcaraz C. Critical Control System Protection in the 21st Century / C. Alcaraz, S. Zeadally // Computer. — 2013. — Vol. 46. — P. 74–83. doi:10.1109/MC.2013.69

УДК 004.056.53:656.078 (045)

Лахно В.А. Повышение кибербезопасности информационно-коммуникационных систем транспорта

Аннотация. *Информационно-коммуникационная среда транспорта (ИКСТ) ориентирована на взаимодействие с другими секторами экономики для сокращения задержек при транспортировке грузов, обработке морских и речных судов, контейнеров, железнодорожных вагонов, автомобилей и др. на основе использования систем электронных накладных, «клиент-банк», e-business и т. п. Критичность выхода из строя систем такого уровня сложности требует новых исследований по обеспечению информационной безопасности (ИБ) ИКСТ. При этом делается акцент на доступность, конфиденциальность и целостность информации, которая хранится и обрабатывается в информационных системах (ИС), автоматизированных системах управления (АСУ) транспорта. Статья содержит результаты исследований, направленных на дальнейшее развитие методов и моделей распознавании угроз ИКСТ и совершенствования ИБ в условиях формирования единого информационно-коммуникационного пространства транспорта, внедрения новых и модернизации существующих ИС и АСУ при увеличении количества дестабилизирующих воздействий на информационные ресурсы. Предложен метод распознавания угроз для информационной безопасности на основе дискретных процедур, позволяющий повысить вероятность распознавания, создавать эффективные аналитические, схемотехнические и программные решения для систем защиты информации.*

Ключевые слова: *информационно-коммуникационная среда транспорта, защита информации, информационная безопасность, распознавание угроз, дискретные процедуры.*

Lakhno V. Increase the cybersecurity of transport information and communications systems

Abstract. *The system approach to solving problems of information security, proposed in this work provides for the integration of mathematical models of the processing and protection of information, connecting invulnerability and flexibility for each of three aspects of security (confidentiality, availability and integrity) of information based on structural unification of these contradictions. The method for modeling the security policy to provide a highly reliable information processing. This paper contains contains the results of studies aimed at further development of methods and models of recognition of threats to information and communications environment of the transport industry (ICETI). A method for intelligent recognition of threats based on the discrete procedures has been first developed, thus allowing creating an effective analysis, hardware and software solutions of the system of information protection ICETI.*

Key words: *systems of transportation and communication, information security, information security, threat detection, mathematical models.*

Отримано *11 січня 2016 року*, затверджено редколегією *1 березня 2016 року*