

МЕТОД ТА МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОМУ СЕРЕДОВИЩУ ТРАНСПОРТУ

Олександр Петров¹, Олександр Корченко², Валерій Лахно³

¹Гірничо-металургійна академія (м. Краків), Польща

²Національний авіаційний університет, Україна

³Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна, Україна



ПЕТРОВ Олександр Степанович, д.т.н.

Рік і місце народження: 1951, селище Горний, Красно-Партизанського району, Саратовської області, РФ.

Освіта: Луганський машинобудівний інститут (з 2001 року Східноукраїнський Національний університет імені Володимира Даля), 1973 рік.

Посада: професор кафедри прикладної інформатики.

Наукові інтереси: інформаційна безпека, безпека інформаційно-комунікаційних систем.

Публікації: більше 250 наукових публікацій, серед яких монографії, навчальні посібники, підручники, наукові статті та патенти на винаходи.

E-mail: petrov@snu.edu.ua



КОРЧЕНКО Олександр Григорович, д.т.н.

Рік і місце народження: 1961, Київ, Україна.

Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет), 1983 рік.

Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.

Наукові інтереси: інформаційна і авіаційна безпека.

Публікації: більше 300 наукових публікацій, серед яких монографії, словники, навчальні посібники, підручники, наукові статті та патенти на винаходи.

E-mail: icaocentre@nau.edu.ua



ЛАХНО Валерій Анатолійович, к.т.н.

Рік і місце народження: 1964, Луганськ, Україна.

Освіта: Луганський машинобудівний інститут (з 2001 року Східноукраїнський Національний університет імені Володимира Даля), 1987 рік.

Посада: доцент кафедри комп'ютерних інформаційних технологій.

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. Робота містить результати досліджень направлених на подальший розвиток методів та моделей інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспортної галузі (ІКСТГ) та удосконаленню інформаційної безпеки в умовах формування єдиного інформаційно-комунікаційного середовища, створення державної єдиної інтегрованої інформаційної системи (ДЄІС), впровадження нових та модернізації існуючих інформаційних систем на транспорті, і збільшення кількості нестабілізуючих впливів на доступність, конфіденційність 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, транспортна галузь.

Вступ

Транспорт є найважливішою та найпотужнішою галуззю будь-якої країни світу. Він виконує в державі важливі економічні, оборонні,

соціально-політичні й культурні функції. Економічна роль транспорту полягає, насамперед, у тому, що він є органічною ланкою кожного виробництва, проводить безперервну й масову

доставку всіх видів сировини, палива й продукції з пунктів виробництва в пункти споживання, а також здійснює поділ праці, спеціалізацію й кооперацію виробництва [1-5].

В Україні транспортна діяльність робить суттєвий внесок для створення валової доданої вартості (ВДВ) – за даними Державної служби статистики України, її частка в 2013 році становила майже 12 %, а вартість основних засобів виробництва (за первинною оцінкою) – 35 % від загальної вартості виробничого потенціалу країни.

Транспортний комплекс України поєднує в собі різні види транспорту, такі як: морський та річковий, автомобільний, залізничний, авіаційний, трубопровідний. Кожен з них має свою специфіку [3, 4].

Інформаційно-комунікаційне середовище транспортної галузі (ІКСТГ), орієнтоване на взаємодію з іншими секторами економіки для скорочення затримок при транспортуванні вантажів, обробці морських та річкових суден, контейнерів, залізничних вагонів і вантажів на прикордонних переходах на основі використання даних електронних накладних, систем клієнт-банк, e-business, систем GSM-R, VSAT, взаємодії із клієнтурою й партнерами тощо.

В рамках державних і міждержавних програм інформатизації створюються сучасні комплекси інформаційних, інформаційно-керуючих систем та автоматизованих систем керування (АСК) транспортної галузі (далі по тексту ІСТГ), а також державна єдина інтегрована інформаційна система (ДЄІС).

Активне розширення ІКСТГ, особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується появою нових загроз для інформаційної безпеки (ІБ), про що свідчить зростання кількості інцидентів (див. рис. 1), пов'язаних із ІБ та захистом інформації, а також виявлених уразливостей у інформаційній системі (ІС) та АСК ТГ. Загрози є цілком реальними, оскільки злочинці можуть отримати можливість перехоплювати паролі, окремі файли, геолокаційну інформацію, транслювати аудіо та відео дані, контролювати Wi-Fi мережі, веб-камери, інформаційні табло на автомобільних та залізничних шляхах, вокзалах, аеропортах, тощо [1, 6, 7-11].

Найбільш серйозними проблемами в області ІБ ІКСТГ залишається його захист від несанкціонованого доступу (НСД), навмисних програмно-технічних впливів на інформацію з метою порушення її конфіденційності, цілісності та доступності в процесі обробки і зберігання. Про серйозність проблеми свідчить хоча б той факт, що навіть одна людина, яка має доступ до даних ІКСТГ, за незначний час може повністю паралізувати роботу будь якого стратегічного залізничного вузла, морського порту, газо- або нафтотранспортного підприємства, мультимодального транспортно-логістичного центру та ін. Для цього достатньо вмонтувати в програмне забезпечення (ПЗ) ДЄІС, ІС або АСК ТГ усього кілька десятків рядків коду

програми-вірусу. Якщо ДЄІС, ІС або АСК ТГ не будуть мати спеціальних засобів захисту, то це загрожуватиме, як мінімум, істотними економічними втратами підприємству, та як максимум, на деякий час зупинкою певних бізнес процесів у транспортній галузі в цілому.

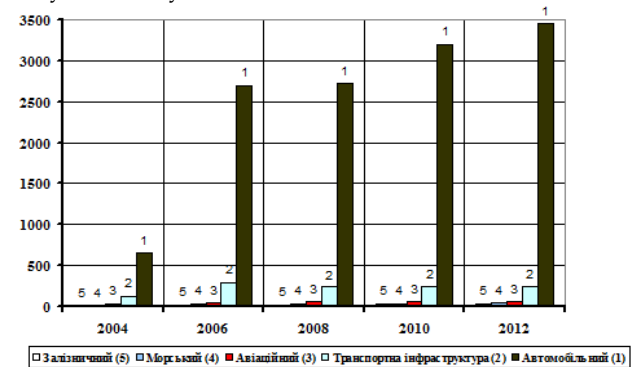


Рис. 1. Загальна кількість інцидентів ІБ на транспорті

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 загроз в межах існуючих та нових класів вторгнень у ІКСТГ.

Категорії елементів ІКСТГ як об'єкти нападу на інформацію

Об'єктом атаки (комп'ютерного нападу на інформацію – КНІ) може стати будь-який з елементів ІКСТГ. Проте в цілому всі елементи ІКСТГ можуть бути віднесені до однієї з трьох категорій (див. рис. 2): центри обробки даних (ЦОД), АСК, АІС, ІС; периферійне обладнання та PLC; системи та канали зв'язку для обміну даними [1,3-5, 11-14].

Перш ніж приступати до питань інформаційної безпеки ДЄІС, ІС та АСК ТГ, необхідно зрозуміти, з яких компонентів вони складаються, які об'єкти слід захищати і від кого.

Для ДЄІС, ІС та АСК ТГ характерними є наступні види елементів: бортові засоби, що встановлюються на рухомих об'єктах ІКСТГ (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.



Рис. 2. Категорії елементів ІКСТГ, як об'єкти нападу на інформацію

До складу технологічного комплексу ДЄІС, ІС та АСК ТГ можуть входити різноманітні технічні системи та засоби: системи і засоби координатно-часового, метеорологічного та інших 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 [4, 5].

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 таких базових характеристик безпеки інформації, як конфіденційність, цілісність або доступність [6, 8].

Після виявлення в промислових та транспортних SCADA та ІС таких складних вірусів як Stuxnet (2010 р.), Duqu (2011 р.), Flame (2012 р.), Careto (2014 р.) відбувся різкий стрибок інтересу до ІБ критично важливих АСК, АІС та ІС. У підсумку в 2011–2013 рр. у компонентах SCADA на транспорті було виявлено більше 70 уразливостей [1-3, 5, 6]. Наприклад, найбільша кількість уразливостей була виявлена у компонентах АСК ТП виробництва компанії Siemens, які широко використовуються в ТГ, зокрема, на залізничному транспорті [2, 5].

Інтерес для зловмисників можуть представляти такі складові АСК ТГ, як системи SCADA та людино-машинний інтерфейс (НМІ), в яких у термін з 2004 – 13 рр. було виявлено більше 120 уразливостей [2, 3, 5] (див. рис. 3).

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 (див. рис. 4) [7, 9, 10].

За даними, представленими в [1, 2, 7, 9] кількість уразливостей в АСК зв'язку та транспорту, з 2004 року збільшилися на 600% (див. рис. 5).

Крім того, як показали дослідження 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 КНІ), частка уразливостей низької складності знизилася з максимального рівня – більш ніж на 90% в 2004 році, до 48% в 2012 році (див. рис. 6).

Тим часом, за той же період уразливості середньої складності збільшили свою частку з 5% до 47%. Розкриття інформації зі складними уразливими залишалося стабільним в останні десятиліття, їх частка в середньому становить всього 4% [2-4].

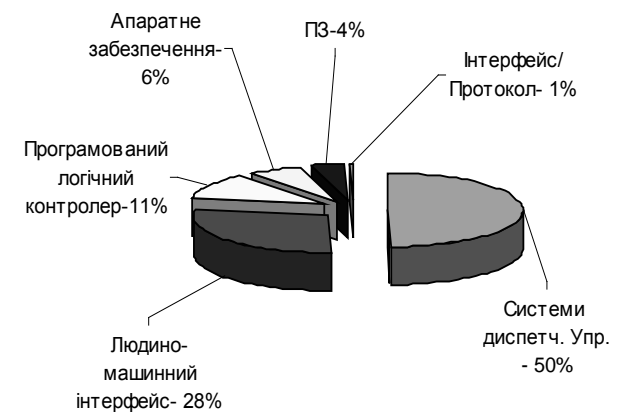


Рис. 3. Загрози для АСК ТГ

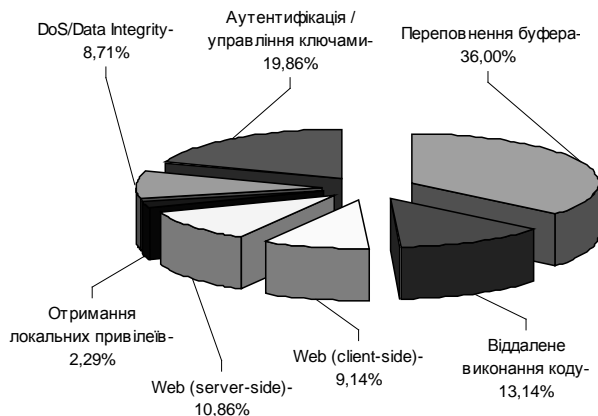


Рис. 4. Типи уразливостей АСК ТТ

У зловмисників є кілька точок входу, щоб скомпрометувати АС або ІС ТТ. Системи АСК ТТ можуть бути заражені різними способами, наприклад, вірус (експлоїт) може бути впроваджений через USB-з'єднання або через мережевий інтерфейс.

Порушення працездатності ІС або АСК ТТ 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 Rwn (Південна Корея). Так, наприклад, в 2013 і 2014 роках учасники повинні були знайти і скористатися уразливими в АСК і отримати доступ до системи управління моделлю залізниці, а також, порушити працездатність автоматичного залізничного переїзду. Система АСК моделлю залізниці була побудована на продуктах компанії Siemens і контроллерах S7-1200. У ході конкурсу вдалося відправити системі помилкові сигнали та в ході спуфінга АСК перестала працювати (DoS).

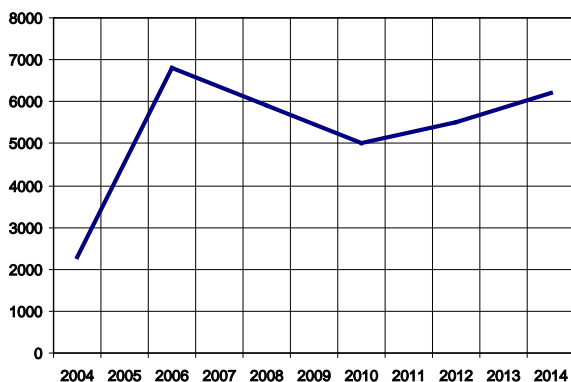


Рис. 5. Динаміка зростання уразливостей в АСК зв'язку та транспорту

На аналогічному конкурсі в Лас-Вегасі (США) хакери з компанії ЮActive продемонстрували можливість DOS-атаки сучасної системи управління автомобільним рухом. В ході атаки було згенеровано фальшиві дані від сенсорів, з яких інформація надходить в центр управління. У разі відмови табло, на автомагістралях утворювалась тиснява та корки.

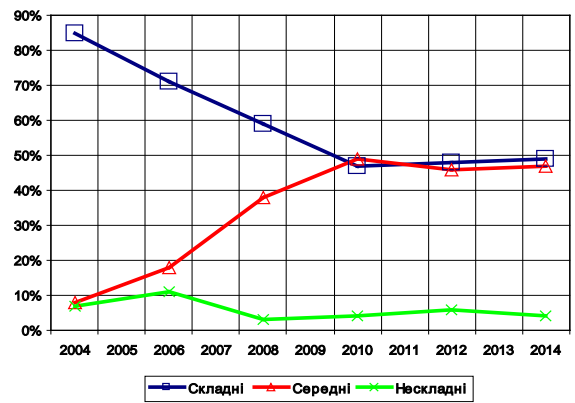


Рис. 6. Необхідна складність атак

На повітряному і морському транспорті загрози ІБ також є досить актуальною проблемою. Хакери взагалі не обов'язково перебувати на борту транспортного засобу. Достатньо отримати контроль над системою управління і відправити екіпажу помилкові команди, або викликати відмову в обслуговуванні системи, генеруючи відомо надлишковий трафік сигналів для бортової АРМ.

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

Формування моделі загроз ІКСТТ

Ступінь небезпеки кожної загрози ІКСТТ залежить від низки чинників, що підвищують або знижують захищеність об'єкту інформаційної безпеки (ОІБ) від загрози певного класу, наприклад, комп'ютерного вторгнення. Чинники, 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 ДІПРЗ ІБ може бути подана в різних формах, зокрема, у вигляді важко з'ясовних ознак НСД $\{p_{ax1}, \dots, p_{axn}\}$ у ДЄПС та ІСТГ, діапазонів граничних значень, параметрів вхідного і вихідного трафіка, непередбачуваних адрес пакетів, атрибутів, часових параметрів, запитів тощо.

Оцінка можливості реалізації загрози залежить від низки чинників. У багатьох джерелах можливість реалізації загрози визначається як певна ймовірність [8-11, 14]. Однак, загроза, яка є джерелом потенційного збитку, а тому є певною небезпекою, будь-яким чином повинна бути виміряна. Фактично, мова йде про формування моделі загроз для ІКСТТ (див. рис. 7).

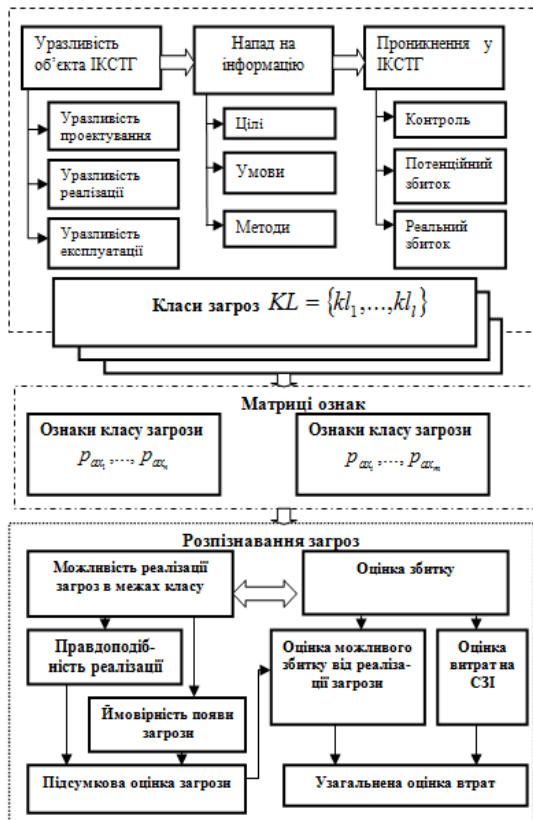


Рис. 7. Взаємозв'язок факторів категорії загроз ІКСТГ

Якщо системи інтелектуального розпізнавання загроз для ІКСТГ ще підлягають своїй реалізації, то формалізована постановка задачі для їх розробки може бути сформульована наступним 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 ІКСТГ (ДЄПС, ІСТГ, АСК та ін.), яка підлягає захисту (топология, 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 тощо; *gov* – вирішальне (розв'язувальне) правило в межах визначеної політики безпеки.

Завдання, які вирішуються СІРЗ можуть бути записані таким чином:

Аналіз захищеності:

$$IOFP_j = FS(SYS, TAI, AT, gov), \quad (2)$$

де $IOFP_j$ – значення *j*-го показника захищеності; *AT* – події ІБ, що відображають напад на інформацію (наприклад, атаку на ДЄПС, ІСТГ, АСК та ін.); *FS* – функція, яка визначає $IOFP_j$ на основі прийнятої ПБ.

Управління кореляцією СІРЗ:

$$K_{event} = FCor\{e_i\}, \quad (3)$$

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

Моделювання атак (нападів на інформацію):

$$ESC_{cr} = Model(SYS, TAI, AT, gov, T), \quad (4)$$

де $ESC_{cr} \in SYS$ – критичний елемент системи; *Model* – модель КНІ у часі – *T*.

Підтримка прийняття рішень (або експертна система):

$$CM = \arg \min |IOFP - IOFP_{requirement}|, \quad (5)$$

де $CM \in gov$ – оптимальний контрзахід (СЗІ), що є елементом вирішального правила в рамках ПБ ТГ; $IOFP$ та $IOFP_{requirement}$ – поточне та еталонне значення показника захищеності, відповідно.

Таким чином, формальна постановка задачі підтримки прийняття рішення (*CM*), є завданням синтезу. Цим вона принципово відрізняється від усіх попередніх, які є завданнями аналізу.

Візуальне представлення даних у випадку розпізнавання загрози ІБ

$$CM_v = FVizual(VF(SYS, Events, gov)), \quad (6)$$

де *VF* – візуальний інтерфейс аналітика СЗІ; *FVizual* – функція візуалізації, яка дозволяє застосовувати контрміру – CM_v .

Безумовно, вимірювання загрози слід почати з оцінки можливості її виникнення. Така оцінка може бути зроблена на основі даних по відомим фактам появи загрози, вираженим через статистичну частотність. Дану оцінку можна розглядати як оцінку, засновану на наявному досвіді експлуатації СЗІ ІКСТГ. Другим фактором оцінки можливості реалізації загрози є оцінка витрат, що неминуче виникають при введенні тих чи інших засобів захисту.

Метод інтелектуального розпізнавання загроз ІКСТГ

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

Існує остаточний набір об'єктів $\{sp_{a1}, \dots, sp_{am}\}$ 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 загрози 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 підписів (або фрагментів описів) об'єктів (див. табл. 1) [5].

Таблиця 1

База знань для інтелектуального розпізнавання загроз ІКСТГ

Атрибути	Ознаки нападу на інформацію	Інформативність значення ознаки	Універсум	Терми для лінгвістичної оцінки $\varphi_u, \dots, \varphi_v$
Множина класів загроз ІБ $KL = \{KL_1, \dots, KL_n\}$, Множина цілей порушника в ІКСТГ $PA = \{PA_1, \dots, PA_2\}$, Множина номерів загроз ІБ, реалізованих порушником при досягненні ра-ої мети $B_{p_a} = \{b_{p_{a1}}, \dots, b_{p_{am}}\}$, Множина номерів ЗЗІ $N_j^{p_a} = \{n_j^{p_{a1}}, \dots, n_j^{p_{am}}\}$, Множина можливих порушників $U = \{u_1, \dots, u_g\}$, Множина зафіксованих інцидентів $NIS = \{nis_1, \dots, nis_f\}$, Множина можливих варіантів нападу $AT = \{AT_1, \dots, AT_q\}$, та ін.	Множина ознак нападу на інформацію в межах класу KL $p_{ax} = \{p_{ax1}, \dots, p_{axm}\}$.	На основі NIS $-1 \leq IZ_{p_{axj}} \leq 1$	$[0, N_a]$ або $[0,1]$, у. о.	некритичний, критичний або виявлені, частково виявлені, невиявлені, невиявлені або зафіксовані СЗІ, незафіксовані СЗІ або уразливості виявлені, частково виявлені, невиявлені, невиявлені тощо.
Стани систем (ДЄПС, ІС та АСК ІТ) $S_{IK} = \{S_{IK_1}, \dots, S_{IK_m}\}$				
Методи протидії (засоби захисту ІКСТГ) $D_{zzi} = \{D_{zzi_1}, \dots, D_{zzi_f}\}$				
Правила для дерева висновку ІФ ($KL_1 \vee \dots \vee KL_n \vee S_{IK_j} \vee \dots \vee S_{IK_m}$) THEN D_{zzi} , та				
$\mu^{d_j}(S_{IK_j}) = \bigvee_{p=1}^{h_j} \left[\mu^{y_1}(y_1) \wedge \dots \wedge \mu^{\varphi_v}(\varphi_v) \right], p = \overline{1, h_j}, j = \overline{1, MI}$, де $\mu^{y_1}(y_1), \dots, \mu^{\varphi_u}(\varphi_u), \mu^{\varphi_v}(\varphi_v)$ - функції належності змінних $y_1, \dots, \varphi_u, \dots, \varphi_v$ до їх нечітких термів; y_1 - стан ІБ {нижче за критичний, критичний, вище за критичний, високий}; \vee - логічне АБО, \wedge - логічне І, як операції max і min, відповідно [15].				

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, \dots, KL_f) 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.

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

У системі ознак $\{p_{a1}, \dots, p_{am}\}$ виділяється сукупність різних підмножин виду

$$NP_{p_a} = \{p_{a1}, \dots, p_{am}\}, r_{p_a} \leq MI. \quad (7)$$

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

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

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

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

$$\Gamma(sp_a, KL) = \frac{1}{|LW_{KL}|} \sum_{sp_{ai} \in KL} \sum_{NP_{p_a} \in \Omega MI} po_{sp_a} \cdot po_{NP_{p_a}} \cdot BN(sp_a, sp_{ai}, NP_{p_a}), \quad (8)$$

де $|LW_{KL}| = |KL \cap \{sp_{a1}, \dots, sp_{am}\}|$. Об'єкт sp_{an} належить до того класу, який має найбільшу оцінку.

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

$$\begin{aligned} \Gamma(sp_{a1}, KL_1) &> \Gamma(sp_{a1}, KL_2), \Gamma(sp_{aMI}, KL_1) > \Gamma(sp_{aMI}, KL_2), \\ \Gamma(sp_{aMI_{i+1}}, KL_2) &> \Gamma(sp_{aMI_{i+1}}, KL_1), \\ &\dots \\ \Gamma(sp_{aMI}, KL_2) &> \Gamma(sp_{aMI}, KL_1). \end{aligned} \quad (9)$$

Рішення системи зводиться до вибору параметрів $ro_{sp_{ai}}$ $i = 1, 2, \dots, PA$, та $ro_{NP_{pa}}$, $NP_{pa} \in \Omega MI$. У разі, якщо система несумісна, знаходиться її максимальна спільна підсистема за рішенням якої визначаються значення параметрів $ro_{sp_{ai}}$ і $ro_{NP_{pa}}$.

Процедура розпізнавання загрози ІКСТГ для об'єкта $sp_a = (\alpha_{p_{a1}}, \dots, \alpha_{p_{aMI}})$, 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_i - певна логічна функція F_{KL} , що ухвалює значення 0 на описах об'єктів $sp_{an} = (\alpha_{p_{an1}}, \dots, \alpha_{p_{anMI}})$ з KL_i і значення 1 на інших наборах з E_{KL}^{MI} , тут E_{KL}^{MI} - множина усіх наборів довжини r_{pa} . Покриттю класу KL_i відповідає припустима для F_{KL} кон'юнкція, тупиковому покриттю - максимальна для F_{KL} кон'юнкція. Припустима (максимальна) кон'юнкція \mathfrak{R} визначає належність об'єкта $sp_{an} = (\alpha_{p_{an1}}, \dots, \alpha_{p_{anMI}})$ класу $(KL_i) = (B_{pa})$, якщо $(\alpha_{p_{a1}}, \dots, \alpha_{p_{aMI}}) \notin NI_{\mathfrak{R}}$.

Побудувати скорочену ДНФ логічної функції можна також шляхом перетворення кон'юнктивної форми вигляду $D_1 \wedge D_2 \wedge \dots \wedge D_u$, де

$D_i = p_{ax1}^{\beta_{i1}} \vee p_{ax2}^{\beta_{i2}} \vee \dots \vee p_{axMI}^{\beta_{iMI}}, i = 1, 2, \dots, mi$ реалізує функцію F_{KL} , β_{iMI} - елементи набору B_{KL} , де

$$p_{ax}^{\alpha} = \bigvee_{\beta_i \neq \alpha_i} p_{ax}^{\beta}$$

Тоді кон'юнктивна форма набуває вигляду

$$D_1^* \wedge D_2^* \wedge \dots \wedge D_u^*, \quad (10)$$

де $D_i^* = \bigvee_{i \neq \beta_{i1}} p_{ax1}^{\eta} \vee \bigvee_{i \neq \beta_{i2}} p_{ax2}^{\eta} \vee \dots \vee \bigvee_{i \neq \beta_{iMI}} p_{axMI}^{\eta}, i = 1, 2, \dots, u$.

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 \mathfrak{R} , 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. 8, 9.

Під час тестування розробленого методу інтелектуального розпізнавання загроз [12, 13], в якості вхідних даних для навчання та тестування

використовувалася база даних KDD Cup Data. Табл. 2 містить результати виявлення атак найбільш поширених КНІ різними методами у порівнянні з ДПРЗ.

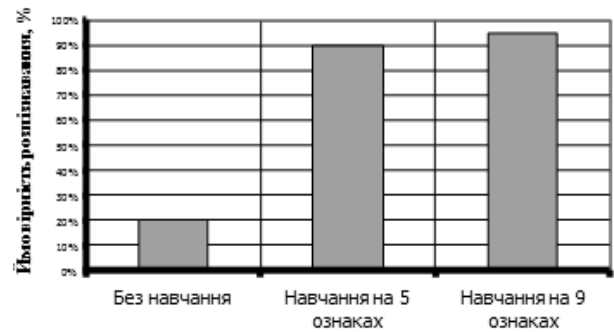


Рис. 8. Ймовірність розпізнавання загрози «НСД до відеосервера»

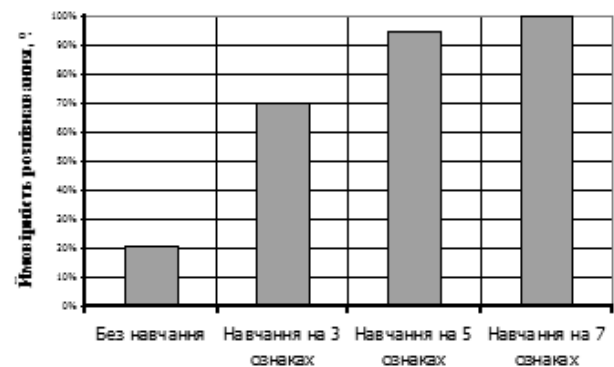


Рис. 9. Ймовірність розпізнавання загрози «НСД до систем супутникової навігації»

Як видно з представлених результатів, запропонований метод ДПРЗ показує кращі результати пошуку КНІ. Слід зазначити, що відсоток помилкових спрацювань, коли легітимне з'єднання приймається за атаку, становить менше 10%. В табл. 5 представлений середні результати відповідно до 4 класів мережевих атак.

Таблиця 2
Результати ІРЗ мережевих атак під час тесту на проникнення

Методи виявлення атак (КНІ)	DoS/DDoS, %	Probe, %	R2L, %	U2R, %
ІРЗ (ДПРЗ)	98,0	95,1	50,5	70,8
Гаусівський класифікатор	82,4	90,2	29,6	22,8
Алгоритм найближчого кластера	97,1	88,8	23,4	22,6
Дерево рішень	97,0	80,8	4,6	10,8

В табл. 3 наведені результати експериментальних досліджень з інтелектуального розпізнавання загроз ІС та АСК підприємств ТОВ «Лугавтотранс» та ІС, АСК депо «Попасна» ДЗ, а також порівняння із результатами імітаційного моделювання, розглянутого у попередньому розділі роботи. Порівняльний аналіз методів розпізнавання загроз ІБ подано в табл. 4.

Таблиця 3

Результати експериментальних досліджень з інтелектуального розпізнавання загроз ІС та АСК підприємств ТГ у порівнянні з імітаційними моделями

№	Параметр	Підприємства ТГ	Імітаційна модель	Відхилення, %
1	Виявлено атак за типами, %: DoS/DDoS (IC, ACK, SCADA, HMI) Probe R2L U2R	92-98 88-95 47-50 67-71	85-96	7-9
2	Ймовірність досягнення зловмисником мети за $T_{зд}=60$ хвилин: DoS/DDoS (IC, ACK, SCADA, HMI) Probe R2L U2R	0,06-0,11 0,05-0,11 0,02-0,07 0,02-0,06	0,08-0,10	0,05-0,10
3	Успішна атака R2L, год	4-8		
4	Успішна атака U2R, год	1-4		

Таблиця 4

Порівняльний аналіз методів розпізнавання загроз ІБ

Алгоритми, які використовуються для розпізнавання	Дерево рішень	Нейронні мережі	Байєсівські мережі довіри	Методи нечіткої логіки	ДПРЗ+ нечіткі бази знань
точність	+/-	-	-	-	-
можливість пояснення	-	+	+	-	-
масштабованість	-	+/-	+/-	+/-	-
швидкодія	+/-	+	+/-	+/-	-
здатність до навчання	+/-	+/-	-	-	-

«+» - наявність труднощів; «-» - відсутність труднощів; «+/-» - часткові труднощі

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 дестабілюючих впливів на інформацію.

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

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] Корниенко А.А. Средства защиты информации на железнодорожном транспорте.

[учеб. пос.] / А.А. Корниенко, М.А. Еремеев, С.Е. Ададунов - М.: Маршрут. - 2006, 256 с.

[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.

[6] MITRE Research Program. [Электронный ресурс]: Режим доступа: <http://www.mitre.org>

[7] The Web Hacking Incidents Database 2008: Annual Report. [Электронный ресурс]: Режим доступа: <http://www.breach.com/confirmation/2008/WHID.html>

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

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

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

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

[12] 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.

[13] Лакно В.А. Экспериментальні дослідження зміни продуктивності корпоративних інформаційних систем підприємств в умовах реалізації комп'ютерних атак / В.А. Лакно, А.С. Петров // Інформаційна безпека. – Луганськ. – 2011. – №1(5). – С. 181-189.

[14] Петров А.С. Вероятностные модели конфликтных потоков данных в системах защиты информации корпоративных сетей / В.А. Лакно,

А.С. Петров, А.С. Ленков // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К. – 2009. – № 22. – С. 99-107.

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

УДК 004.056.53:656.078 (045)

Петров А.С., Корченко А.Г., Лакно В.А. Метод и модель интеллектуального распознавания угроз информационно-коммуникационной среде транспорта

Аннотация. Работа содержит результаты исследований направленных на дальнейшее развитие методов и моделей интеллектуального распознавания угроз информационно-коммуникационной среде транспортной отрасли (ИКСТО) и совершенствованию информационной безопасности в условиях формирования единого информационно-коммуникационной среды, создание государственной единой интегрированной информационной системы, внедрение новых и модернизации существующих информационных систем на транспорте и увеличение количества дестабилизирующих воздействий на доступность, конфиденциальность и целостность информации. Разработан метод интеллектуального распознавания угроз на основе дискретных процедур с использованием аппарата логических функций и нечетких множеств, который позволяет повысить эффективность распознавания угроз ИКСТО, создавать эффективные аналитические, схемотехнические и программные решения СЗИ ИКСТО.

Ключевые слова: защита информации, информационная безопасность, интеллектуальное распознавание угроз, дискретные процедуры, нечеткие множества, транспортная отрасль.

Petrov O., Korchenko O., Lakhno V. Method and model of intellectual threats detection for information and communication transport environment

Abstract. The work contains research results aimed at further development of methods and models for information and communication environment transport sector intellectual threat detection and information security improvement in the emerging unified information-communication environment, creating a single integrated state information system, 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. A method of predictive threat detection based on discrete procedures using the apparatus of logic functions and fuzzy sets, which allow to increase the efficiency of threats detection, create effective analysis, hardware and software solutions.

Key words: information security, intellectual threats detection, discrete procedures, fuzzy sets, transport.

Отримано 25 лютого 2015 року, затверджено редколегією 12 березня 2015 року
