УДК 004.056.53:656.078

В. А. Лахно, д-р техн. наук

КІБЕРБЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ ТРАНСПОРТУ

Анотація. *Запропонована модель оцінки загроз для кібербезпеки інформаційних систем транспорту в умовах збільшення кількості дестабілізуючих впливів на доступність, конфіденційність і цілісність інформації. Розглянута задача прийняття рішень для забезпечення кібербезпеки інформаційних систем наземного транспорту на основі нечіткого регресійного механізму висновку про загрози кібератак.*

Ключові слова: кібербезпека, наземний транспорт, інформаційні системи, уразливість, кібератака, модель, нечітка логіка, інформаційна безпека

В. А. Лахно, д-р техн. наук

КИБЕРБЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ ТРАНСПОРТА

Аннотация. *Предложена модель оценки угроз для кибербезопасности информационных систем транспорта в условиях увеличения количества дестабилизирующих воздействий на доступность, конфиденциальность и целостность информации. Рассмотрена задача принятия решений для обеспечения кибербезопасности информационных систем наземного транспорта на основе нечеткого регрессионного механизма вывода об угрозах кибератак.*

Ключевые слова: *кибербезопасность, наземный транспорт, информационные системы, уязвимость, кибератака, модель, нечеткая логика, информационная безопасность*

V. Lakhno, ScD.

CYBER SECURITY OF COMPUTER SYSTEMS OF TRANSPORT

Abstract. *The results of researches, allowing raising the level of protection of the information systems of transport enterprises are presented in the article. Using the new mathematical models of flexible reliability, availability, confidentiality and integrity of information processed, allowing mathematically describe the mechanisms of cyber security.*

Keywords: *cyber safety, land transport, information systems, vulnerability, cyber-attack, model, fuzzy logic, information security*

Вступ. Сьогодні в транспортній галузі України розвивається ряд галузевих інформаційних систем (ІС) і мереж зв'язку, що працюють автономно, і не взаємопов'язані одна з одною. Наприклад, на залізничному транспорті використовуються наступні системи: автоматизована система керування (АСК) пасажирськими перевезеннями (АСК ПП УЗ); АСК вантажними перевезеннями (АСК ВП УЗ-Є); АСК електронним документообігом Укрзалізниці (АС СКЕДО); автоматизована система самообслуговування (АСС) «е-Квиток»; автоматизована система контролю вантажів та цілісності залізничних вагонів у русі (АСК ЦВР). На автотранспорті використовуються АСК: «АвтоГраф»; "Wialon Hosting"; "Fort Monitor 3" та ін. На морському та річковому транспорті впроваджені: Єдина інформаційна система портового співтовариства; річкова інформаційна система. На повітряному транспорті багато років існує корпоративна система управління на базі ERP Державного підприємства обслуговування повітряного руху України та ін. Типова структура ІС на транспорті, являє собою сукупність локальних вузлів (ЛВ), що є пунктами концентрації інформації та об'єднані одним ЛВ спеціального виду, який реалізує ретрансляцію інформаційних потоків і є центром керування доступом (ЦКД). ЛВ можуть представляти собою ІС, групи ІС, окремі компоненти систем (база даних, клієнт-додаток, сервер-додаток) або групи компонентів та відповідні механізми захисту [1; 2].

Втручання в національні, регіональні й муніципальні комп'ютерні системи транспорту (КСТ) часто згадувана загроза для кібератак зловмисників [3-6]. Об'єктом атаки може стати будь-який з елементів КСТ. В цілому всі елементи інформаційно-

комунікаційного середовища транспорту до однієї з трьох категорій: центри обробки даних (ЦОД); АСК та ІС; периферійне обладнання; системи та канали зв'язку для обміну даними.

Мета. Метою даної роботи є апробація нових моделей розпізнавання кіберзагроз для КСТ, які, на відміну від існуючих, дозволяють прийняти остаточне рішення про наявність або відсутність загрози в межах існуючих та нових класів кібератак на ІКСТ.

Кібербезпека комп'ютерних систем транспорту. Практично кожна КСТ може виступати об'єктом кібератаки. Після виявлення в промислових та транспортних АСК та ІС таких складних вірусів як Stuxnet (2010 р.), Duqu (2011 р.), Flame (2012 р.), Careto (2014 р.) відбувся різкий стрибок інтересу до кібербезпеки (КБ) критично важливих АСК та ІС. У підсумку в 2011-2015 р. у компонентах АСК на транспорті було виявлено більше 75 вразливостей [7]. Найбільша кількість уразливостей (42) за звітний період було виявлено у компонентах АСК виробництва компанії Siemens, які широко використовуються в КСТ, наприклад, на залізничному транспорті [1; 2].

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 [6; 7].

За даними, представленими в [6; 7; 8] кількість уразливостей у КСТ, з 2004 року збільшилися на 600%.

Крім того, як показало дослідження [3; 4; 5; 7], вимоги до рівня складності для успішного проведення кібератаки проти КСТ, а також систем зв'язку (після того як зловмисник отримав доступ до цілі атаки), частка уразливостей низької складності знизилася з (ІКСТ) можуть бути віднесені максимального рівня - більш ніж на 90% в 2004 році, до 45% в 2014 році.

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% [6]. КСТ 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 [6; 7], тобто, це в вісім разів більше, ніж за період з 2005 р. по 2010 р.

Не варто скидати з рахунків і DDoS/DoS атаки на АСК, в результаті яких знижується рівень кібербезпеки [8].

Порушення працездатності КСТ 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 [9; 10]. Модель КС управління залізницею була побудована на продуктах компанії Siemens і контролерах S7-1200. У ході конкурсу вдалося відправити КС помилкові сигнали та в ході спуфинга АСК перестала працювати (DoS).

На аналогічному конкурсі в Лас-Вегасі (США) хакери з компанії IOActive продемонстрували можливості DoS атаки на КС 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 утворювалися пробки [1; 6].

На повітряному і морському транспорті загрози КБ також може стати досить актуальною проблемою. Хакеру взагалі навіть 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 свідомо надлишкова трафік сигналів для бортової ЕОМ.

Уразливість КСТ обумовлена відсутністю механізмів безпеки в промислових протоколах і системах відповідно до проекту, уразливістю ПЗ та його некоректною конфігурацією [1; 2; 8]. Необхідність інтеграції з зовнішніми мережами (корпоративними, WAN, Інтернет), використання бездротових мереж і відкритих інформаційних технологій - ОС, мережевих протоколів і служб, віддаленого доступу - теж не сприяють безпеці КСТ.

Модель системи розпізнавання загроз кібератак. У разі можливого впливу на інфраструктурні об'єкти нашої країни з боку вороже налаштованих держав, терористичних або злочинних організацій, одним з найбільш вразливих місць інфраструктури є транспорт. Рівень загроз зростає у зв'язку з розвитком і впровадженням КСТ, наприклад, Укрзалізниця вже зараз займається розробкою єдиної комплексної системи управління рухом високошвидкісних поїздів Інтерсіті.

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:

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

де SYS - дані про інфраструктуру КСТ, яке підлягає захисту (топологія, склад елементів, користувачі, методи та засоби кіберзахисту та ін.); $Events$ - дані про події КБ, які пройшли попередню обробку і знаходяться в базі знань на зберіганні; TAI - дані про сценарії кібератак у вигляді шаблонів [2-4]; 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) КСТ [2; 6].

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

Аналіз захищеності КСТ:

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

де $IOFP_j$ - значення j - го показника захищеності; AT - події пов'язані із порушенням кібербезпеки (КБ), що відображають кібератаку; FS - функція яка визначає $IOFP_j$ на основі прийнятої ПБ.

Моделювання кібератак:

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

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

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

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

де $CM \subset gov$ - оптимальний контрзахід (система захисту інформації - СЗІ), що є елементом вирішального правила в рамках ПБ КСТ; $IOFP$ та $IOFP_{\text{r}}$ - поточне та еталонне значення показника захищеності КСТ, відповідно.

Загроза зміни стану КБ КСТ 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 КСТ - um^* (потенційні уразливості); SDN - множина суб'єктів КСТ; 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^*.

Вирішальне правило gov формулюється на основі нечіткого регресійного механізму

висновку про загрози кібератак на базі розробленого методу інтелектуального розпізнавання загроз [2; 6; 10], суть якого полягає у визначенні кон'юнкцій за покриттям класів загроз ІБ КСТ. 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 КСТ.

Результати дослідження. Запропонований підхід, заснований на застосуванні методу дискретних процедур розпізнавання загроз (ДПРЗ) [10], дозволяє значно підвищити рівень виявлення мережевих кібератак у КСТ. Виявлення більшості типів мережевих атак відбувається з ймовірністю 75-98 % при незначному рівні помилкових спрацювань. Крім цього, запропонований метод не вимогливий до ресурсів КСТ і здатний виявляти невідомі типи кібератак.

Під час проведення тесту на проникнення та для тестування розробленої експертної системи було проведено низку експериментів для ІС транспорту. В якості вхідних даних для навчання та тестування використовувалася база даних KDD Cup Data [3; 4; 6; 10].

В ході тестів для розробленого методу розпізнавання кібернападів були отримані наступні результати [6, 10]:

для атак DoS/DDoS - для помилок першого роду (кількість помилкових спрацьовувань) - 10,2%) і помилок другого роду (кількість невиявлених атак) - 2,9%;

для атак Probe - для помилок першого роду - 12,1% і помилок другого роду - 3,1%;

для атак R2L - для помилок першого роду - 9,4% і помилок другого роду - 2,7%;

для атак U2R - для помилок першого роду - 11,3% і помилок другого роду - 3,4%.

Висновки. Як показали результати дослідження найбільшої уваги потребують такі компоненти захисту КСТ, як системи протидії кібератакам у ІКСТ. З'ясовано, що складність застосування до систем розпізнавання загроз кібератак у КСТ формалізованого апарату аналізу й синтезу систем захисту, полягає в тому, що конкретна КСТ і його підсистема кібербезпеки складаються з різнорідних елементів, які описуються з використанням різних математичних моделей. Показано, що застосування елементів адаптивного захисту інформації може бути засноване на використанні новітніх методів та моделей інтелектуального розпізнавання загроз кібербезпеці ІКСТ.

Список використаної літератури

1. Корниенко А.А. Средства защиты информации на железнодорожном транспорте : учебное пособие [Текст] / А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров. – Москва: Маршрут, 2006. – С. 256.

2. Lahno V. A. Modeling information security system of transport enterprises [Text] / V.A. Lahno // Management and production engineering : monography / M. Dudek, H. Howaniec, A. Petrov, etc. - Bielsko-Biala, 2012. Chapter V. – pp. 221-248.

3. Vacca John R. Managing Information Security : an introduction [Text] / R. John Vacca. – Elsevier. Syngress, 2010. – pp. 320. ISBN: 978-1-59749-533-2

4. Сайт организации "Mitre" [Электронный ресурс]. Режим доступа: http://www.mitre.org /research /overview (дата доступа (01.02.2016).

5. Сайт компании "Trustwave" [Электронный ресурс]. Режим доступа: https://www.trustwave.com/Resources/Security-Stats/ (дата доступа 30.01.2016).

6. Lahno V. Ensuring of information processes' reliability and security in critical application data processing systems [Text] / V. Lahno // MEST Journal. – Belgrade. – 2014. – Vol. 2, No 1. - pp. 71–79.

7. Сайт организации "Scadahacker" [Электронный ресурс]. Режим доступу: https://www. scadahacker.com/ (дата доступа 01.12.2015).

8. SANS Institute InfoSec Reading Room. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis [Электронный ресурс] : Режим доступу: https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-

implementation-detailed-analysi-33764 (дата доступа 01.06.2014).

9. Хакерские соревнования на Positive Hack Days: [Электронный ресурс]: Режим доступу: https://habrahabr.ru/company/pt/ blog/ 178439/ (дата доступа 30.04.2013).

10. Lahno V. Information security of critical application data processing systems [Text] / V. A. Lahno // TEKA. Commission of motorization and energetics in agriculture. – 2014. - Vol. 14, No.1, P. 134-143.

Получено 10.02.2016

References

1. Kornienko A.A., Yeremeev M.A., Adadurov S.Ye. Sredstva zashchity informatsii na zheleznodorozhnom transporte. [The means of protection information in rail transport], (2006), Moscow, *Marshrut Publ.*, pp. 256 (In Russian).

2. Lahno V. A., Petov A.S. Modeling information security system of transport enterprises. Management and production engineering: monography / Edited by M. Dudek, H. Howaniec. Poland, Bielsko-Biala, Academia Techniczno – Humanistyczna w Bielsko-Biala, (2012), pp. 221-248 (In English).

3. Vacca J.R., (2010), Managing Information Security, USA, *Elsevier-Syngress*, pp. 320 ISBN: 978-1-59749-533-2 (In English).

4. Website of "Mitre" [Electronic Resource] (In English), available at: http://www.mitre.org /research /overview (accessed 01.02.2016).

5. Website of "Trustwave" [Electronic Resource] (In English), available at: https://www.trustwave.com /Resources/ Security-Stats/ (accessed 30.01.2016).

6. Lahno V. Ensuring of information processes' reliability and security in critical application data processing systems (2014), *MEST Journal*, Belgrade, Serbia, Vol. 2, No 1, pp. 71-79. (In English).

7. Website of "Scadahacker" [Electronic Resource] (In English), available at: https://www. scadahacker.com/ (accessed 01.12.2015).

8. SANS Institute InfoSec Reading Room, Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis, [Electronic Resource] (In English), available at: https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764 (accessed 01.06.2014).

9. Khakerskie sorevnovaniya na Positive Hack Days, [Hacking contest in the Positive Hack Days] [Electronic Resource] (In Russian), available at: https://habrahabr.ru/company/pt/ blog/ 178439 / (accessed 30.04.2013).

10. Lahno V. Information security of critical application data processing systems, (2014), *TEKA. Commission of motorization and energetics in agriculture*, Krakow, Poland, Vol. 14, No.1, pp. 134-143 (In English).

Лахно
Валерій Анатолійович,
д. т. н., доц. зав. каф. Організації комплексного захисту інформації ПВНЗ «Європейський університет»
Тел.:(044)-276-52-51
E-mail:Valss21@ukr.net