КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.113122
УДК 004.056

Лахно Валерій Анатолійович
Д.т.н., професор, зав. кафедрою комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0001-9695-4543
Valss21@ukr.net

Блозва Андрій Ігорович
К.пед.н., доцент, доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0002-4377-0916
Andriy.blozva@nubip.edu.ua

Місюра Максим Дмитрович
К.т.н., доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0002-9061-3462
Mdm@nubip.edu.ua

Касаткін Дмитро Юрійович
К.пед.н., доцент, доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0002-2642-8908
D.kasatkin@nubip.edu.ua

Гусєв Борис Семенович
К.т.н., доцент, доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0003-1658-7822
Gusevbs@nubip.edu.ua

МОДЕЛЬ ПОКАЗНИКА ПОТОЧНОГО РИЗИКУ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ СИСТЕМАМ

Анотація. В статті запропонована модель для оцінювання кількісного показника поточних ризиків реалізації загроз та кібератак на інформаційно-комунікаційні системи транспорту (ІКСТ). Модель відрізняється від існуючих можливістю враховувати ступінь впливу кожної загрози або кібератаки в межах класу на імовірність виникнення аварійної ситуації, що виникає при кібератаках на компоненти інформаційно-комунікаційних систем транспорту, які у багатьох випадках, можна віднести до критично важливих комп'ютерних систем. Показано, що поточні ризики можуть бути незначними, якщо всі потенційно небезпечні параметри інформаційно-комунікаційних систем транспорту підтримуються у встановлених межах, або збільшуватися, набуваючи загрозливого характеру, при відхиленні таких параметрів від норми. Обґрунтовано необхідність описувати ступінь поточної небезпеки ризиків реалізації загроз та кібератак за допомогою деякого кількісного показника. Значення цього показника може залежати від відхилень параметрів, пов'язаних із кібернетичною безпекою інформаційно-комунікаційних систем транспорту. Запропонована відповідна розрахункова формула, для визначення поточного ризику реалізації загрози для інформаційно-комунікаційних систем транспорту. Для апробації запропонованої моделі було проведено імітаційний експеримент, результати, якого теж наведені у статті. Імітаційне моделювання також проведено для перевірки адекватності запропонованої моделі та алгоритму оцінки показника поточних ризиків для компонентів інформаційно-комунікаційних систем транспорту. При цьому враховано, що багато компонентів

інформаційно-комунікаційних систем транспорту працюють у реальному масштабі часу. Показано, що запропонована модель враховує поточні значення метрик інформаційної безпеки та нових класів кіберзагроз для інформаційно-комунікаційних систем транспорту.

Ключові слова: інформаційно-комунікаційні системи транспорту, математична модель, показник поточних ризиків, кібербезпека, захист інформації.

1. ВСТУП

Інформаційна безпека та кібербезпека інформаційно-комунікаційних систем транспорту (ІКСТ) вимагає обліку всіх подій, які відбуваються. Зокрема подій в процесі яких цифрова інформація створюється, модифікується, до неї виконується доступ або вона передається [1], [2]. Реалізація даних заходів є вимогою міжнародного стандарту ISO/IEC 27001:2005 «Системи управління інформаційною безпекою. Вимоги».

Необхідність використання систем моніторингу інформаційної безпеки (ІБ) у ІКСТ визначається тим, що застосування звичайних засобів і механізмів захисту інформації виявляється недостатнім [3]. Зокрема, тому що вони виконують лише базові функції і не дозволяють контролювати безпеку функціонування систем в умовах постійних модифікацій кібератак. Існуючі системи моніторингу безпеки ІКСТ не здатні проводити комплексну оцінку дій зловмисників, будувати послідовність реалізованих уразливостей, визначати кінцеву ціль дій зловмисників і оцінювати ризики реалізації загроз для безпеки ІКСТ, що може привести до повторних успішних атак, а також до фінансових втрат.

Існуючи засоби моніторингу ІБ, наприклад, Intruder Alert, realsecure Network Sensor [3] – [5] та ін., мають певні недоліки:

- Високий рівень помилок першого і другого роду, тобто помилок не визначення кібератак, коли воно має місце, та формування ситуації «атака» при її відсутності;
- Відсутність можливості адаптивно керувати системою ІБ та проводити випереджувальні дії.

Зниження ризиків несанкціонованого доступу (НСД) до інформаційних ресурсів ІКСТ може бути досягнуте вирішенням завдання оцінки й аналізу поточної небезпеки процесу КНІ в реальному часі, щоб завчасно попередити напад і тим самим запобігти розвитку несприятливого сценарію розвитку даної ситуації. Очевидно, що для врахування впливу великої кількості параметрів аномалій та кібератак на ступінь ІБ ІКСТ, а також їх взаємозв'язки систем в реальному масштабі часу, необхідні спеціальні методи й відповідні організаційні, технічні та програмні засоби. Отже тема дослідження є релевантною.

Аналіз останніх досліджень і публікацій. Аналіз попередніх досліджень дозволив визначити перелік потенційних поточних ризиків, що дозволяє визначити найбільш актуальні для ІКСТ загрози та заходу протидії їм, а також оптимізувати вартісні витрати на побудову системи захисту [5] – [7].

Одним із найпоширеніших методів оцінки ризику є метод, заснований на моделі системи «з повним перекриттям», що представляє собою тріаду «загрози – засобу захисту інформації – об'єкти захисту» у вигляді тридольного графа [8], [9].

При проведенні оцінки ризику можна виділити три постановки завдання, що відображають цілі такої оцінки:

1) Оцінка ризику на об'єктах ІКСТ, необладнаних сучасними засобами захисту інформації (ЗЗІ), з метою з'ясування необхідності створення комплексів систем захисту інформації (СЗІ).
2) Оцінка ризику реалізації кіберзагроз з метою модернізації існуючих комплексів СЗІ.
3) Оцінка ризику з метою створення нового комплексу СЗІ.

Необхідно відмітити, що певна кількісна характеристика небезпеки несанкціонованого доступу (НСД) до ІКСТ уже була введена в нормативній документації й у дослідженнях ряду авторів [3], [6], [8], [10]. Відповідно до цих джерел, як кількісна характеристика небезпеки проникнення в ІКСТ розглядається ризик, вимірюваний, як правило, у грошових одиницях, що для критично важливих систем не завжди має першорядне значення.

Отже, потрібно розраховувати ризик для всіх трьох постановок завдання проектування. Урахування реальних зв'язків загроз і ресурсів призводить до того, що ризик необхідно визначати з урахуванням значень елементів матриці зв'язків, значення якої рівні 0 – якщо загроза не може впливати на ресурс, і рівні 1 – якщо загроза потенційно може впливати на інформаційний ресурс.

Мета статті. Розробити модель оцінювання показника поточного ризику реалізації загроз інформаційно-комунікаційного середовища транспорту.

Для вирішення даного завдання в роботі передбачається виконати наступне:

1) Одержати кількісний показник поточних ризиків (ППР) реалізації загроз ІКСТ;
2) Розробити алгоритми оцінки ППР для компонентів ІКСТ, що працюють у реальному масштабі часу, з урахуванням поточних значень метрик інформаційної безпеки та нових класів кібернетичних загроз.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Поточні ризики та загрози кібератак або несанкціонованого проникнення є показниками технологічних процесів в ІКСТ, які можуть набувати різних значень залежно від різних факторів [7].

Інтуїтивно зрозуміло, що поточні ризики можуть бути незначними, якщо всі потенційно небезпечні параметри ІКСТ підтримуються у встановлених межах, або збільшуватися, набуваючи загрозливого характеру, при відхиленні таких параметрів від норми. Тому виникає необхідність описати ступінь поточної небезпеки ризиків реалізації загроз кібератак за допомогою деякого кількісного показника, значення якого залежало б від відхилення параметрів, пов'язаних із ІБ.

Уведення такого показника дозволить здійснювати непрямий вимір ступеня поточних ризиків реалізації загрози кібератаки на ІСКТ.

Ми пропонуємо ввести спеціальний показник для кількісної характеристики ступеня поточної небезпеки атаки або НСД у ІКСТ, який може бути розрахований (виміряний) у будь-який момент часу, зокрема, із використанням методів інтелектуального розпізнавання загроз [7], [10]. Результати вимірів показника можуть бути представлені системному адміністраторові (адміністраторові СЗІ) або використані для вирішення інших завдань.

Якщо процеси у ІКСТ характеризуються ризиками реалізації загроз ІБ, усі значення яких лежать у зоні припустимих значень ZS_0 (див. Рис. 1), то поточна ІБ може

вважатися нульовою. У разі якщо один або кілька параметрів переходять у зону небезпечних значень ZS_1, то поточна небезпека збільшується, і вона буде зростати з наближенням параметрів до зони критичних значень ZS_2.

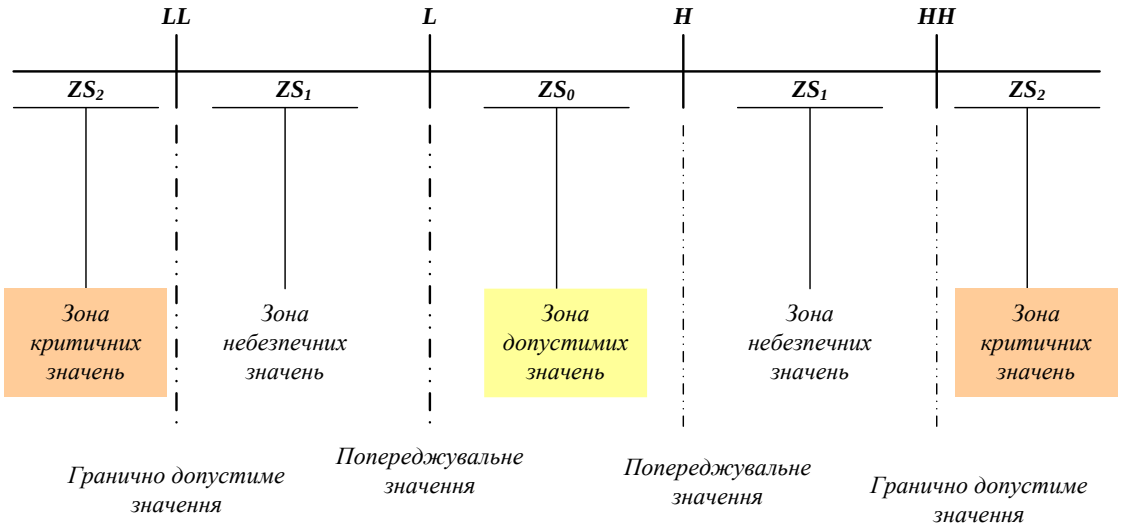

Рис. 1. Ризики реалізації загроз інформаційній безпеці ІКСТ

Зрозуміло, що поточна небезпека проникнення в ІКСТ повинна залежати від загального числа загроз інформації – MI, що одночасно перебувають у зоні ZS_1, від ступеня наближення кожного параметра до зони ZS_2 і від ступеня впливу кожної загрози на можливість виникнення позаштатної ситуації, наприклад, одержання доступу до ресурсів ІКСТ.

3. МЕТОДИКА ДОСЛІДЖЕННЯ

Позначимо ППР через $C_{CRI} = C_{CRI}(\overline{X})$, де $\overline{X}_{CRI} = (x_{CRI\,1},...,x_{CRI\,i},...,x_{CRI\,MI})$ – вектор значень ППР, MI – число загроз інформації.

Показник поточних ризиків C_{CRI} повинен відповідати таким вимогам.

1. Бути скалярною безрозмірною величиною, що змінюється від 0 до 1 ($C_{CRI} = (0 \div 1)$) з урахуванням алгоритмів розпізнавання аномалій та загроз ІБ [9].

2. Бути функцією параметрів x_{CRIi} $C_{CRI} = f((x_{CRI1},...,x_{CRIi},...,x_{CRI\,M})$.

3. Значення C_{CRI} повинні залежати від значень усіх ризиків реалізації загроз для компонентів і процесів в ІКСТ, коли вони перебувають у зоні небезпечних значень $0 < C_{CRI} < 1$,

$$\begin{aligned} &if \quad \exists(x_{CRIi}) : ZS_i = ZS_1,\ i = 1..MI; \\ &or \quad \exists(x_{CRI\,i}) : (x_{CRI\,ill} > x_{CRI\,i} > x_{CRI\,il}) \vee \\ &\vee (x_{CRI\,ih} > x_{CRI\,i} > x_{CRI\,ihh}), \end{aligned} \tag{1}$$

Де $x_{CRI\,il}, x_{CRI\,ih}$ – попереджувальні значення параметрів,

$x_{CRI\,ill}, x_{CRI\,ihh}$ – гранично припустимі значення параметрів.

4. Значення ППР ІБ ІКСТ дорівнює нулю, якщо всі параметри інформаційних процесів в ІКСТ, перебувають у зоні допустимих значень $C_{CRI} = 0$,

$$if \quad \forall(\mathrm{x}_{CRI\,\mathrm{i}}) : ZS_i = ZS_0,\ i = 1..MI.$$

5. Значення ППР дорівнює одиниці, якщо хоча б один технологічний параметр ІКСТ (див. [7], [10], [11]) перебуває в зоні критичних значень $C_{CRI} = 1$,

$$if \quad \exists(\mathrm{x}_{CRI\,\mathrm{i}}) : ZS_i = ZS_2,\ i = 1..MI. \tag{2}$$

6. Значення C_{CRI} Повинне бути зростаючою функцією своїх аргументів.

Якщо $C_{CRI\,1}$ – значення показника C_{CRI} при $x_{CRI\,i} = x_{CRI\,1}$, $C_{CRI\,2}$ – значення показника C_{CRI} при $x_{CRI\,j} = x_{CRIj}1$, і якщо ступінь впливу $x_{CRI\,i}$ буде менше ніж ступінь впливу $x_{CRI\,j}$ то $C_{CRI\,1} < C_{CRI\,2}$.

7. Значення C_{CRI} повинне зростати зі збільшенням числа загроз та атак – даних про інциденти з ІБ у зонах ZS_1 і ZS_2.

Якщо $C_{CRI\,1}$ – значення показника C_{CRI} при $x_{CRI\,i} = x_{CRI\,i}1, \quad ZS_i = ZS_1$, $C_{CRI\,2}$ – значення показника C_{CRI} при

$$\begin{aligned} &x_{CRI\,i} = x_{CRI\,i}1, \\ &x_{CRI\,j} = x_{CRI\,j}1, \\ &ZS_i = ZS_1, \\ &ZS_j = ZS_1\ else \quad C_{CRI\,1} < C_{CRI\,2}. \end{aligned} \tag{3}$$

8. Показник C_{CRI} повинен враховувати ступінь впливу кожної загрози в межах класу KL_i на можливість виникнення аварійної ситуації, що виникає при атаці на компоненти ІКСТ.

Якщо $C_{CRI\,1}$ – значення показника C_{CRI} при $x_{CRI\,i} = x_{CRI}1$, $C_{CRI\,2}$ – значення показника C_{CRI} при $x_{CRI\,j} = x_{CRIj}1$, і якщо ступінь впливу $x_{CRI\,i}$ буде менше, ніж ступінь впливу $x_{CRI\,j}$, то $C_{CRI\,1} < C_{CRI\,2}$.

9. Значення C_{CRI} повинне бути застосовне в будь-якому режимі функціонування ІКСТ. Розрахунки ППР НСД у ІКСТ проводяться за такою залежністю:

$$C_{CRI}(\overline{X}) = \sqrt{\frac{x_{CRI1}^2}{\prod_{i=2}^{MI}(1 + x_{CRIi}^2)} + \sum_{i=2}^{MI} \frac{x_{ПППРi}^2}{\prod_{k=i}^{MI}(1 + x_{CRIk}^2)}}. \tag{4}$$

ISSN 2663 - 4023

Формула обчислення значення C_{CRI} при використанні в ІКСТ вимагає спеціального алгоритму нормування та впорядкування параметрів MI .

Дослідження алгоритму й основних властивостей ППР проведене за допомогою програмного пакету Mathcad.

Припустимо, що кожний C_{CRI} може мати одну або дві зони небезпечних значень (*H – high* і *L – low*).

Якщо параметр $x_{CRI\,i}$ $\left(1 \le i \le MI\right)$ має одну або дві зони небезпечних значень, то перетворення його поточного значення в нормовану величину θ_{i} виконується за формулою (5):

$$\theta_i = \begin{cases} 1, & if \quad \text{x}_{CRI\,\text{i}} \le x^{ll}_{CRI\,i}, \\ \dfrac{x_{CRI\,i} - x^{ll}_{CRI\,i}}{x^{l}_{i} - x^{ll}_{i}}, & if \quad \text{x}^{ll}_{CRI\,\text{i}} < x_{CRI\,\text{i}} < x^{l}_{CRI\,i}, \\ 0, & if \quad \text{x}^{\text{l}}_{CRI\,\text{i}} \le x_{CRI\,\text{i}} \le x^{h}_{CRI\,i}, \\ \dfrac{x_{CRI\,i} - x^{h}_{CRI\,i}}{x^{hh}_{CRI\,i} - x^{h}_{CRI\,i}}, & if \quad \text{x}^{h}_{CRI\,\text{i}} < x_{CRI\,\text{i}} < x^{l}_{CRI\,i}, \\ 1, & if \quad \text{x}_{CRI\,\text{i}} > x^{hh}_{CRI\,i}, \end{cases} \tag{5}$$

Де $\text{x}_{CRI\,\text{i}}$ – поточне значення параметра; $x^{l}_{CRI\,i}, x^{h}_{CRI\,i}$ – попереджувальні значення параметра; $x^{ll}_{CRI\,i}, x^{hh}_{CRI\,i}$ – гранично припустимі значення параметра.

Ступінь впливу кожного з факторів на можливість реалізації загрози ІБ при відхиленні цього параметра від норми, задається шляхом ранжирування, тобто присвоєння параметру певного коефіцієнта (рангу). Ранг параметра K_r представляє собою додатну цілочисельну величину: $K_r = 1, 2, \ldots$. Модель була перевірена під час імітаційного експерименту.

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На рис. 2, 3 наведені, як приклад, залежності ППР C_{CRI} від значень параметрів $\text{x}_{CRI\,\text{i}}$ і θ_i для $MI = 1, 2$ і $K_r = 1, 2$ (наприклад, викрадення ключів для системи зв'язку GSM-R і організація dos/ddos атаки на систему керування рухом поїздів).

У результаті аналізу цих та інших залежностей які були отримані під час імітаційного експерименту, а також досліджених у роботах [5], [7], [10], було зроблено такі висновки:

1. $C_{CRI} = 0$, якщо все θ_i рівні 0;

2. $C_{CRI} = 1$, якщо хоча б один параметр із θ_i рівний 1;

3. $0 < C_{CRI} < 1$, якщо хоча б один параметр із θ_i більше нуля й менше 1 (відповідний параметр x_i перебуває в небезпечній зоні);

4. Якщо при знаходженні одного або декількох параметрів у небезпечній зоні ще один параметр теж потрапляє в небезпечну зону, то показник C_{CRI} зростає;

5. Якщо кількість поточних загроз ІБ $MI=1$ і $K_{r1}=1$, то $C_{CRI} = \theta_1$, тобто показник небезпеки C_{CRI} пропорційний параметру θ_1;

6. Якщо $MI=1$ і $K_{r1}=2$, то залежність C_{CRI} від θ_1 нелінійна. У цьому випадку C_{CRI} більше, ніж при $K_{r1}=1$ для тих самих значень θ_1;

7. Якщо $MI>1$, то всі залежності C_{CRI} від θ_1 нелінійні. При цьому значення показника C_{CRI} тим вище, чим більше параметрів перебувають у небезпечній зоні;

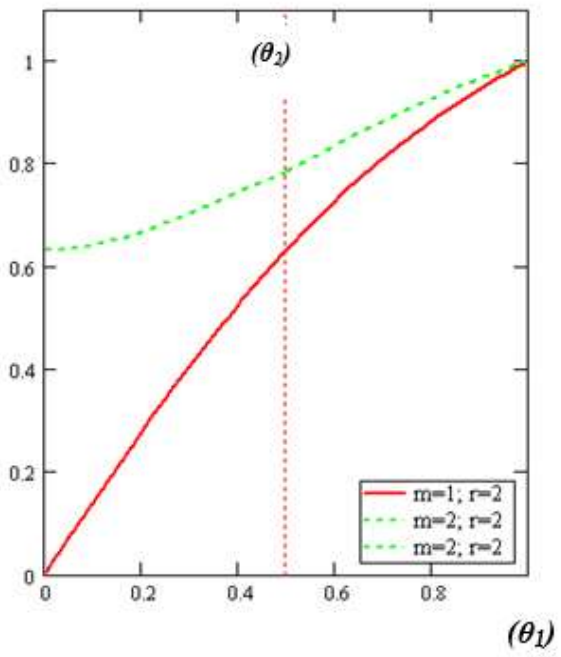

Рис. 2. Залежності $C_{CRI\,i}(\theta_1)$
Для MI=1 і 2 і $Kr_1 = Kr_2 = 2$

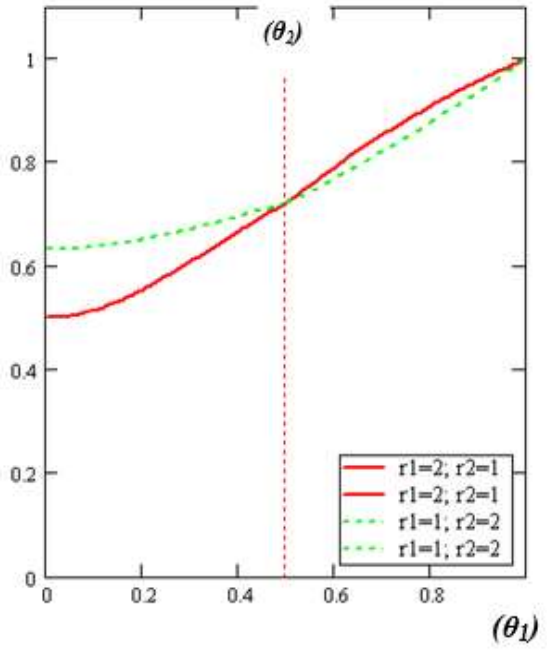

Рис. 3. Залежності $C_{CRI\,i}(\theta_1)$
для MI=2, $Kr_1 > Kr_2$ *і* $Kr_1 < Kr_2$

8. Чим вище ранг параметрів, що перебувають у небезпечній зоні, тим вище показник C_{CRI} за інших рівних умов.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, за результатами проведених досліджень було отримано наступні результати:

- Розроблена модель для оцінювання кількісного показника поточних ризиків реалізації загроз та кібератак на інформаційно-комунікаційні системи транспорту (ІКСТ), яка відрізняється від існуючої можливістю ураховувати ступінь впливу кожної загрози або кібератаки в межах класу на імовірність виникнення аварійної ситуації, що виникає при кібератаках на компоненти ІКСТ;

- Проведено імітаційне моделювання для перевірки адекватності запропонованої моделі та алгоритму оцінки показника поточних ризиків для компонентів ІКСТ, що працюють у реальному масштабі часу, з урахуванням поточних значень метрик інформаційної безпеки та нових класів кіберзагроз для ІКСТ.

Певним недоліком роботи на цьому етапі дослідження є недостатня апробація результатів. Але наші дослідження продовжуються та із часом їх результати буде наведено у наступних публікаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Al Hadidi, M., Ibrahim, Y. K., Lakhno, V., Korchenko, A., Tereshchuk, A., & Pereverzev, A. (2016). Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport. International Review on Computers and Software, 11(12), pp. 1167-1177.

[2] Alcaraz, C., Zeadally, S. (2013). Critical control system protection in the 21st century, Computer, 46 (10), pp. 74-83. DOI: https://doi.org/10.1109/MC.2013.69

[3] Vacca, J.R. (2010). Managing Information Security, Syngress, p. 320.

[4] Lopez, I., Aguado, M. (2015). Cyber security analysis of the European train control system, IEEE Communications Magazine, 53 (10), pp. 110-116. DOI: https://doi.org/10.1109/MCOM.2015.7295471

[5] Lakhno, V., & Hrabariev, A. (2016). Improving the transport cyber security under destructive impacts on information and communication systems. Eastern-European Journal of Enterprise Technologies, 1(3), 4, pp. 4-11. DOI: https://doi.org/10.15587/1729-4061.2016.60711

[6] Dunn, W. (2002). Practical Design of Safety-Critical Systems, Reliability Press, Cambridg.

[7] Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, Eastern-European Journal of Enterprise Technologies, Vol. 2, Iss. 9, 2016, pp. 18-25. DOI: https://doi.org/10.15587/1729-4061.2016.66015

[8] Beketova, G. S., Akhmetov, B. S., Korchenko, A. G. Etc. (2017). Optimization backup model for critical important information systems. Bulletin of the national academy of sciences of the republic of Kazakhstan, (5), pp. 37-44.

[9] Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs, Journal of Theoretical and Applied Information Technology, Vol. 95, Iss. 21, pp. 5778-5786.

[10] Lakhno, V., Zaitsev, S., Tkach, Y. Etc. (2019). Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, 1st International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2018; Kiev; Ukraine; 18 January 2018, Vol. 754, pp. 673-682. DOI: https://doi.org/10.1007/978-3-319-91008-6_66

[11] Akhmetov, B., Lakhno, V., Akhmetov, B., Alimseitova, Z. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 2nd Computational Methods in Systems and Software, comesyso 2018; Szczecin; Poland; 12 September 2018, Vol. 860, pp. 162-171. DOI: https://doi.org/10.1007/978-3-030-00184-1_15

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Valeriy Lakhno
Professor, National University of Life and Environmental Sciences of Ukraine,
Departmentof Computer systems and networks, Kyiv, Ukraine
ORCID: 0000-0001-9695-4543
Valss21@ukr.net

Andriy Blozva
National University of Life and Environmental Sciences of Ukraine,
Departmentof Computer systems and networks, Kyiv, Ukraine
ORCID: 0000-0002-4377-0916
Andriy.blozva@nubip.edu.ua

Maksym Misiura
National University of Life and Environmental Sciences of Ukraine,
Departmentof Computer systems and networks, Kyiv, Ukraine
ORCID: 0000-0002-9061-3462
Mdm@nubip.edu.ua

Dmytro Kasatkin
National University of Life and Environmental Sciences of Ukraine,
Departmentof Computer systems and networks, Kyiv, Ukraine
ORCID: 0000-0002-2642-8908
D.kasatkin@nubip.edu.ua

Borys Gusev
National University of Life and Environmental Sciences of Ukraine,
Departmentof Computer systems and networks, Kyiv, Ukraine
ORCID: 0000-0003-1658-7822
Gusevbs@nubip.edu.ua

MODEL OF CURRENT RISK INDICATOR OF IMPLEMENTATION OF THREATS TO INFORMATION AND COMMUNICATION SYSTEMS

Abstract. The article proposes a model for estimating the quantitative indicator of current risks of threats and cyber attacks on transport information and communication systems (TICS). The model differs from the existing one in taking into account the degree of impact of each threat or cyber attack within the class on the probability of an accident that occurs during cyberattacks on components of transport information and communication systems, which in many cases can be attributed to critical computer systems. It is shown that the current risks may be insignificant if all potentially dangerous parameters of transport information and communication systems are maintained within the established limits, or increase, becoming threatening, when such parameters deviate from the norm. The necessity to describe the degree of current danger of risks of threats and cyberattacks with the help of some quantitative indicator is substantiated. The value of this indicator may depend on the deviations of the parameters related to the cyber security of information and communication systems of transport. An appropriate calculation formula is proposed to determine the current risk of the threat to information and communication systems of transport. To test the proposed model, a simulation experiment was conducted, the results of which are also presented in the article. Simulation modeling was also performed to verify the adequacy of the proposed model and the algorithm for estimating the current risk indicator for components of transport information and communication systems. It is taken into account that many components of transport information and communication systems work in real time. It is shown that the proposed model takes into account the current values of information security metrics and new classes of cyber threats for transport information and communication systems.

Keywords: information and communication transport systems, mathematical model, current risk indicator, cybersecurity, information protection.

REFERENCES

[1] Al Hadidi, M., Ibrahim, Y. K., Lakhno, V., Korchenko, A., Tereshchuk, A., & Pereverzev, A. (2016). Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport. International Review on Computers and Software, 11(12), pp. 1167-1177.

[2] Alcaraz, C., Zeadally, S. (2013). Critical control system protection in the 21st century, Computer, 46 (10), pp. 74-83. DOI: https://doi.org/10.1109/MC.2013.69

[3] Vacca, J.R. (2010). Managing Information Security, Syngress, p. 320.

[4] Lopez, I., Aguado, M. (2015). Cyber security analysis of the European train control system, IEEE Communications Magazine, 53 (10), pp. 110-116. DOI: https://doi.org/10.1109/MCOM.2015.7295471

[5] Lakhno, V., & Hrabariev, A. (2016). Improving the transport cyber security under destructive impacts on information and communication systems. Eastern-European Journal of Enterprise Technologies, 1(3), 4, pp. 4-11. DOI: https://doi.org/10.15587/1729-4061.2016.60711

[6] Dunn, W. (2002). Practical Design of Safety-Critical Systems, Reliability Press, Cambridg.

[7] Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, Eastern-European Journal of Enterprise Technologies, Vol. 2, Iss. 9, 2016, pp. 18-25. DOI: https://doi.org/10.15587/1729-4061.2016.66015

[8] Beketova, G. S., Akhmetov, B. S., Korchenko, A. G. Etc. (2017). Optimization backup model for critical important information systems. Bulletin of the national academy of sciences of the republic of Kazakhstan, (5), pp. 37-44.

[9] Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs, Journal of Theoretical and Applied Information Technology, Vol. 95, Iss. 21, pp. 5778-5786.

[10] Lakhno, V., Zaitsev, S., Tkach, Y. Etc. (2019). Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, 1st International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2018; Kiev; Ukraine; 18 January 2018, Vol. 754, pp. 673-682. DOI: https://doi.org/10.1007/978-3-319-91008-6_66

[11] Akhmetov, B., Lakhno, V., Akhmetov, B., Alimseitova, Z. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 2nd Computational Methods in Systems and Software, comesyso 2018; Szczecin; Poland; 12 September 2018, Vol. 860, pp. 162-171. DOI: https://doi.org/10.1007/978-3-030-00184-1_15