КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.5160
УДК 004.491/.492 -049.5 : 656.1/.5

Лахно Валерій Анатолійович
д.т.н., професор, завідувач кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0001-9695-4543
valss21@ukr.net

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

Смолій Віктор Вікторович
к.т.н., доцент, доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0003-2834-6989
dr.v.smoliy@gmail.com

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

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

Осипова Тетяна Юріївна
к.пед.н., доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0002-9199-3436
t_osipova@nubip.edu.ua

МЕТОДИ СИСТЕМНОГО АНАЛІЗУ ПРИ ФОРМУВАННІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

Анотація. Викладено підходи до застосування методів системного аналізу для вирішення задач пов'язаних із забезпеченням інформаційної безпеки підприємств на транспорті, які відрізняються складною ІТ структурою з великою кількістю компонентів. Показано, що активне розширення областей інформатизації транспортної галузі, особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується появою нових загроз інформаційної безпеки. Показано, що для побудови ефективної системи інформаційної безпеки, вибору і впровадження адекватних технічних засобів захисту повинен передувати етап опису, аналізу та моделювання загроз, вразливостей, з подальшим розрахунком ризиків для ІБ і визначенням оптимальної стратегії розвитку системи інформаційної безпеки (СІБ). Після оцінки різних варіантів СІБ за декількома критеріями, приймається рішення: якщо рекомендації збігаються, то з більшою впевненістю обирається оптимальне рішення. Якщо спостерігається протиріччя висновків експертів, то остаточне рішення приймається з урахуванням його переваг і недоліків, наприклад, вибирається та стратегія розвитку системи інформаційної безпеки, яка виявилася оптимальною хоча б для двох критеріїв. Якщо отримані різні стратегії розвитку СІБ для всіх трьох критеріїв, то потрібно варіювати значеннями показника песимізму-оптимізму в критерії Гурвіца або змінити дані, наприклад, про можливі загрози для ІС або

автоматизованої системи управління підприємства. Запропоновано алгоритм моделювання процесу прийняття рішення щодо вибору оптимальної стратегії управління інвестиційним проектуванням компонентами системи інформаційної безпеки для господарюючого суб'єкта на транспорті.

Ключові слова: інформаційна безпека; методи системного аналізу; критерії оцінки системи інформаційної безпеки.

ВСТУП

В останні роки в багатьох країнах використовується практика, коли в рамках державних програм інформатизації на транспорті 0, 2, створюються мультитехнологічні системи інформаційної безпеки (СІБ) для АСУ (автоматизовані системи управління) і АІС (автоматичні інформаційні системи), що інтегрують нормативні, апаратні і програмні елементи захисту. Активне розширення областей інформатизації транспортної галузі, особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується появою нових загроз безпеки, про що свідчить статистика інцидентів **Ошибка! Источник ссылки не найден.**,3, яка показувала, що АІС транспортних підприємств (АІСТП) піддаються агресивним програмним впливам незалежно від якості і складності застосовуваних заходів захисту. Нанесений збиток визначається економічними втратами, пов'язаними з простоями устаткування, непередбачуваними порушеннями у виробничих процесах, необхідністю відновлювальних процедур, наслідками реалізації загроз щодо цінної інформації, об'єктів інформатизації і, у підсумку, суспільства в цілому. Дана проблема є характерною для всіх критично важливих інформаційних систем, експлуатованих на різних рівнях інформатизації: від АСУ рухом до продажу електронних квитків.

Постановка проблеми. Розробка методики формування загальної стратегії забезпечення інформаційної безпеки (ІБ) на транспорті і, зокрема, її складових частин - управлінської та технічної політики.

Аналіз останніх досліджень і публікацій. Проблема забезпечення безпеки різних ІС на транспорті посилюється відсутністю єдиної методичної бази, що дозволяє проводити адекватну оцінку загроз інформаційним ресурсам, а також ступеня захищеності даних. Поки що, найбільш популярним напрямком є підхід на основі оцінки та управління ризиками **Ошибка! Источник ссылки не найден.**-5. Необхідність системного аналізу ІБ на етапах проектування і експлуатації АІС викликана неприпустимо низьким рівнем ефективності існуючих засобів забезпечення ІБ. Так, наприклад, за статистичними даними Національного відділення ФБР США з комп'ютерних злочинів, «величина імовірності запобігання несанкціонованого проникнення в ІС складає в середньому близько 0,12-0,15» 6. У той же самий час «у багатьох прикладних галузях, де забезпеченню безпеки процесів і об'єктів приділяється серйозна увага, норми безпеки, викладені у відповідних документах, мають порядок 0,9» 6.

Основний матеріал статті. На щорічних (2000-2019 р.) світових конгресах Міжнародного союзу автотранспортників (МКАТ) відзначалась важливість розвитку і вдосконалення глобальних інформаційних технологій бізнесу для оптимізації транспортного процесу 0, 7, 8. Було зроблено висновок про необхідність переходу від конкуренції між видами транспорту до активної співпраці на основі мультимодальності і транспортної логістики 0.

Підвищення ефективності прийняття управлінських рішень, в тому числі в питаннях інформаційної безпеки, можливо за рахунок консолідації інформаційних ресурсів транспортної галузі в єдине ціле. Прикладом слугують центри ситуаційного управління (ЦСУ) на різних видах транспорту, АІС яких дозволяють зберігати дані про операційну діяльність, здійснювати їх опрацювання і подальший аналіз з метою підвищення ефективності бізнес процесів 2, 7, 8.

Слід зауважити, що застосування методів системного аналізу дає результат, тільки в тих випадках, коли використання цих методів пов'язане з вибором відповідної математичної моделі. Останнє твердження не означає, що в даний час знайдені адекватні математичні моделі СІБ АІС. Хоча і отримані кількісні результати для АІС на основі застосування теорії черг, ТМО, тощо в області опису моделей даних. Проте, важко собі уявити можливість написання єдиної математичної моделі АІС, в якій би враховувалися всі проблеми, пов'язані з забезпеченням ІБ і захисту інформації.

Відповідно до положень системного аналізу необхідні моделі СІБ, що дозволяють описувати: структуру системи; механізми її функціонування і поведінки (прояв механізмів функціонування в оточуючих умовах, що змінюються).

При розробці таких моделей необхідно врахувати наступні обмеження:

1. На даний час не представляється можливим описати СІБ АІС єдиною математичною моделлю.

2. Моделювання СІБ АІС передбачає використання елементів опису системи на природній мові. Такі моделі прийнято називати семантичними моделями, в зв'язку з тим, що зміст елементів моделі визначається їх іменами.

3. Якщо і можливе моделювання ІС, то тільки сукупністю пов'язаних моделей.

Розглянемо загальну постановку питання системного аналізу ІБ АІС. Для такого аналізу необхідно представити деяку СІБ, що складається з компонентів, кожен з яких представляє собою безліч відносно однорідних елементів, об'єднаних функціями, що дозволяють забезпечити виконання загальних цілей СІБ (див. Рис. 1.).

Перший елемент СІБ - це комплекс нормативно-методичних документів (КНМ), що містить вимоги з безпеки до всіх процесів опрацювання інформації.

Другий - це організаційна структура ІБ, що представляє собою з про сукупність організаційних рішень по забезпеченню ІБ на транспорті.

Третій елемент СІБ - інфраструктура ІБ, яка утворюється деякою сукупністю технічних рішень щодо забезпечення ІБ і захисту інформації.

Для СІБ мають місце такі компоненти:

- стратегії (способи) захисту інформації;
- стратегії (методи) прогнозування нападу на об'єкт, що розглядається;
- механізми прийняття рішення, що використовують результати обох стратегій і представляють собою політику безпеки (набір норм, правил і практичних прийомів, що регулюють управління і розподіл цінної інформації).

Наприклад, організація захисту інформації в найзагальнішому вигляді може бути сформульована як задача пошуку оптимального компромісу між потребами в захисті і необхідними ресурсами для цих цілей 9, 10. Потреби обумовлені важливістю (конфіденційністю, комерційною цінністю) і обсягами інформації що захищається, умовами її зберігання, передачі, опрацювання і використання. Ресурси можуть бути обмежені заданою межею або визначаються умовою обов'язкового досягнення необхідного рівня захисту, що вимагається. У першому випадку захист організовується так, щоб при виділених ресурсах забезпечувався максимальний рівень захисту, а в другому - рівень захисту забезпечує мінімальне витрачання ресурсів.

Рис. 1. Структура системи інформаційної безпеки

Неважко помітити, що сформульовані випадки є не що інше, як пряма і зворотна постановки оптимізаційних задач. Вони достатньо детально вивчені за допомогою методів сучасної теорії систем, інформатики і прикладної математики. Однак, наявні невизначені ситуації, а також, перш за все, в даному випадку неможливість отримання функціональних залежностей між обсягом витрачених ресурсів і рівнем захисту, що досягається не дозволяють строго вирішити ці завдання подібними відомими методами. Тому, з метою створення умов для орієнтації в цих невизначених ситуаціях і вводиться поняття стратегії захисту 11.

Під нею розуміється системний погляд на ситуацію, що склалася, який поширюється і на системний підхід до прийняття найбільш раціонального рішення в цій ситуації.

У загальному випадку формальну математичну модель СІБ *S* можна представити у вигляді такої множини величин, які описують процес її функціонування.

Введемо наступні позначення:

$x_i \in X$, $i = \overline{1, n_X}$ – сукупність вхідних впливів на СІБ;

$y_j \in Y$, $j = \overline{1, n_Y}$ – сукупність вихідних характеристик СІБ;

$v_k \in V$, $k = \overline{1, n_V}$ – сукупність вхідних впливів на СІБ з боку зовнішнього середовища;

$s_l \in S$, $l = \overline{1, n_S}$ – сукупність внутрішніх параметрів СІБ.

Отже, формальна модель системи може бути описана наступним чином

ISSN 2663 - 4023

$$\begin{cases} y_1(\tau) = f_1(x_1, x_2, ..., x_{n_X}, v_1, v_2, ..., v_{n_V}, s_1, s_2, ..., s_{n_S}, \tau); \\ y_2(\tau) = f_2(x_1, x_2, ..., x_{n_X}, v_1, v_2, ..., v_{n_V}, s_1, s_2, ..., s_{n_S}, \tau); \\ .....; \\ y_{n_V}(\tau) = f_{n_V}(x_1, x_2, ..., x_{n_X}, v_1, v_2, ..., v_{n_V}, s_1, s_2, ..., s_{n_S}, \tau), \end{cases} \quad (1)$$

де τ- час.

Якщо розглядати процес функціонування СІБ як послідовну зміну її станів: $\vec{S}(\tau_1), \vec{S}(\tau_2), ..., \vec{S}(\tau_k)$, то вони можуть бути інтерпретовані як координати точок в *k* - мірному фазовому просторі.

Формально стан СІБ (*S)* в момент часу $\tau_0 < \tau^* \le T$ повністю визначається її початковим станом $\vec{S} = \vec{S}(\tau_0)$, сукупністю вхідних впливів на СІБ $\vec{X}(\tau^*)$, керуючими впливами $\vec{U}(\tau^*)$, вхідними впливами на СІБ з боку зовнішнього середовища $\vec{V}(\tau^*)$, які проходили за проміжок часу $\tau^* - \tau_0$.

Стани СІБ можуть бути описані наступними векторними рівняннями:

$$\begin{cases} \vec{S}(\tau) = g(\vec{S}^0, \vec{X}, \vec{V}, \vec{U}, \tau); \\ \vec{y}(\tau) = f(\vec{S}, \tau). \end{cases} \quad (2)$$

Перше рівняння за початковим станом СІБ S_0 і змінними $\vec{X}, \vec{V}, \vec{U}$ визначає вектор-функцію $\vec{S}(\tau)$, а друге за станом $\vec{S}(\tau)$ визначає ендогенні змінні на вході системи $\vec{y}(\tau)$.

Будь-яка АІСТП має *M* параметрів безпеки $\{z_1, ..., z_M\}$, де для всіх $w = 1, M$ z_w належить деякій множині $\sum_w$ (носію *w*-го параметру). У реальних системах число параметрів безпеки дуже велике (наприклад, для операційних систем значення *M* перевищує 1000).

Розглянемо приклад використання методів системного аналізу під час обрання засобів захисту ІС (АІС) від потенційних мережевих атак [12].

На першому етапі необхідно сформувати вихідні дані. Формується матриця параметрів $X = \|x_i\|$. Формується множина допустимих стратегій розвитку СІБ $C = \{C_D\}, d \in \overline{1,q}$, де *q* - кількість і кість стратегій.

Для *d*-ой стратегії C_d визначаються значення критеріїв:

Вальда $WA_d = \min_j y_{dj}, d \in \overline{1,q};$

Севіджа $SE_d = \max_{d \in \overline{1,q}} y_{di} - y_{dj};$

Гурвіца $GU = \max_{d \in \overline{1,q}} (\beta \cdot \min_{j \in \overline{1,m}} y_{dj} + (1-\beta) \cdot \max_{j \in \overline{1,m}} y_{dj},$

де фіксоване значення $\beta \in [0;1]$, m – кількість станів навколишнього середовища, яке впливає на кількість загроз для ІС (АІС) підприємства.

Далі формується вектор значень результатів (WA_d, SE_d, G_d). На завершальному етапі розраховується гарантоване найменше значення ризику застосування *d*-ої стратегії в найгіршій ситуації для критеріїв:

Вальда $\mathrm{R}_{\mathrm{d_{WA}}} = \max\limits_{d\in\overline{1,q}} WA_d$;

Севіджа $\mathrm{R}_{\mathrm{d_{SE}}} = \min\limits_{d\in\overline{1,q}} \max\limits_{j\in\overline{1,m}} SE_d$;

Гурвіца $R_{d_{GU}} = \max\limits_{d\in\overline{1,q}} GU_d$,

де $\mathrm{R}_{\mathrm{d_{WA}}}$ - індекс стратегії по Вальду $\left(d_{WA} \in \overline{1,q}\right)$;

$\mathrm{R}_{\mathrm{d_{SE}}}$ - індекс стратегії по Севіджу $\left(d_{SE} \in \overline{1,q}\right)$;

S_{k_G} - індекс стратегії по Гурвіцу $\left(d_{GU} \in \overline{1,q}\right)$.

Далі формується $\left(\mathrm{ST}_{\mathrm{opt}}\right)$ оптимальна стратегія розвитку СІБ у відповідності з наступними умовами :

$$\begin{cases} якщо\ \mathrm{R}_{\mathrm{d_{WA}}} = \mathrm{R}_{\mathrm{d_{SE}}} = \mathrm{R}_{\mathrm{d_{GU}}},\ то\ \mathrm{ST}_{\mathrm{opt}} = \mathrm{R}_{\mathrm{d_{WA}}}; \\ \begin{cases} якщо\ (\mathrm{R}_{\mathrm{d_{WA}}} = \mathrm{R}_{\mathrm{d_{GU}}}) \vee (\mathrm{R}_{\mathrm{d_{WA}}} = \mathrm{R}_{\mathrm{d_{SE}}}) \vee (\mathrm{R}_{\mathrm{d_{SE}}} \neq \mathrm{R}_{\mathrm{d_{GU}}}), \\ то\ \mathrm{ST}_{\mathrm{opt}} = \mathrm{R}_{\mathrm{d_{WA}}}; \\ якщо\ (\mathrm{R}_{\mathrm{d_{WA}}} = \mathrm{R}_{\mathrm{d_{GU}}}) \vee (\mathrm{R}_{\mathrm{d_{WA}}} \neq \mathrm{R}_{\mathrm{d_{SE}}}) \vee (\mathrm{R}_{\mathrm{d_{SE}}} = \mathrm{R}_{\mathrm{d_{GU}}}), \\ то\ \mathrm{ST}_{\mathrm{opt}} = \mathrm{R}_{\mathrm{d_{GU}}}; \\ якщо\ (\mathrm{R}_{\mathrm{d_{WA}}} \neq \mathrm{R}_{\mathrm{d_{GU}}}) \vee (\mathrm{R}_{\mathrm{d_{WA}}} = \mathrm{R}_{\mathrm{d_{SE}}}) \vee (\mathrm{R}_{\mathrm{d_{SE}}} = \mathrm{R}_{\mathrm{d_{GU}}}), \\ то\ \mathrm{ST}_{\mathrm{opt}} = \mathrm{R}_{\mathrm{d_{SE}}}; \end{cases} \\ якщо\ \mathrm{R}_{\mathrm{d_{WA}}} \neq \mathrm{R}_{\mathrm{d_{SE}}} \neq \mathrm{R}_{\mathrm{d_{GU}}},\ то\ змінюються\ вихідні\ дані. \end{cases} \quad (3)$$

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пропонований алгоритм являє собою детальну послідовність етапів моделювання процесу прийняття рішення щодо вибору оптимальної стратегії управління інвестиційним проектуванням компонентами СІБ для господарюючого суб'єкта на транспорті.

Відповідно до запропонованого алгоритму проведемо вибір обладнання для запобігання комп'ютерних атак.

Таблиця 1

Матриця ймовірностей реалізації комп'ютерних атак

Тип атаки	**Імовірність використання різних типів атак**	**Варіанти використання засобів захисту (ЗасЗ)**						
		ЗасЗ відсутні (0)	**Fire-wall (1)**	**Засоби виявлення вторгнення (2)**	**Резервні канали зв'язку і сервер (3)**	(1) + (2)	(1) + (3)	(1) + (2) + (3)
		Імовірність відбиття атаки/Пропорційна вартість ЗасЗ (у.о.)						
Smurf-ping	0,31	0,0/0	0,7/1	0,8/50	0,8/20	0,92/51	0,9/21	0,98/71
ICMP flood	0,1	0,0/0	0,8/1	0,95/50	0,83/20	0,97/51	0,87/21	0,995/71
UDP flood	0,14	0,0/0	0,8/1	0,95/50	0,8/20	0,96/51	0,85/21	0,98/71

TCP flood	0,11	0,0/0	0,8/1	0,99/50	0,8/20	0,99/51	0,9/21	0,999/71
TCP SYN flood	0,31	0,0/0	0,6/1	0,935/50	0,75/20	0,95/51	0,8/21	0,98/71

Для отриманих розрахункових значень критеріїв Вальда, Гурвіца і Севіджа можуть бути отримані графічні залежності з використанням пакета MatLab 2019. На рис.2 наведено графік залежності при використанні критерію Вальда.

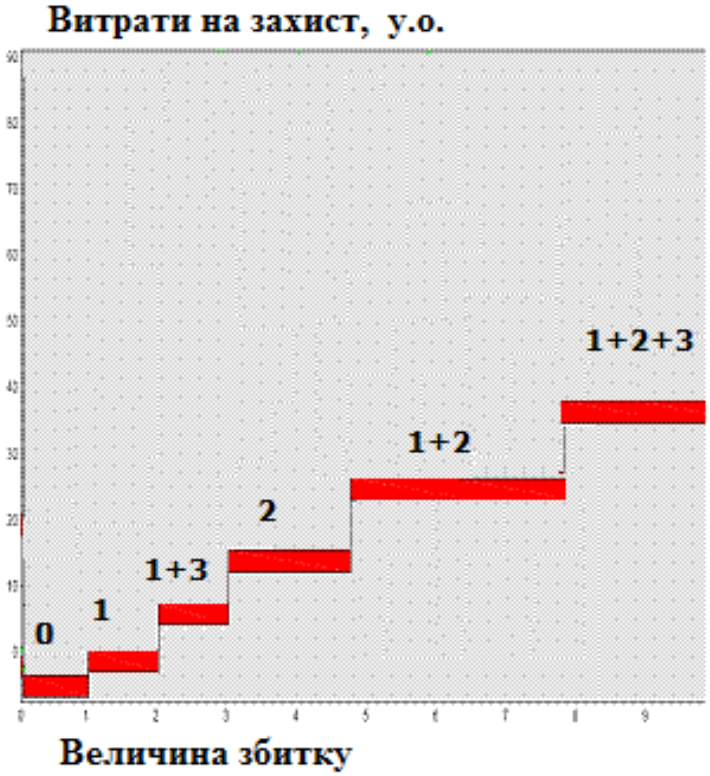

Рис. 2. Графік залежності вартості Зас3 від величини передбачуваного збитку з використанням критерію Вальда

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Для побудови ефективної системи інформаційної безпеки, вибору і впровадження адекватних технічних засобів захисту повинен передувати етап опису, аналізу та моделювання загроз, вразливостей, з подальшим розрахунком ризиків для ІБ і визначенням оптимальної стратегії розвитку СІБ. Після оцінки різних варіантів СІБ за декількома критеріями, приймається рішення: якщо рекомендації збігаються, то з більшою впевненістю обирається найкраще рішення. Якщо спостерігається протиріччя висновків експертів, то остаточне рішення приймається з урахуванням його переваг і недоліків, наприклад, вибирається та стратегія розвитку СІБ, яка виявилася оптимальною хоча б для двох критеріїв. Якщо отримані різні стратегії розвитку СІБ для всіх трьох критеріїв, треба варіювати значеннями показника песимізму-оптимізму в критерії Гурвіца або змінити дані, наприклад, про можливі загрози для ІС (АІС) підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Conference of Ministers of Transport (ECMT). http: // international transport forum.org/pub/pdf/06Europe-AsiaRU.pdf
2. Transport informatization: Best examples. http://www.cnews.ru/news/top/index.shtml?2013/02/11/518663
3. Volynskaya, A. V. (2004). *Increasing the stability of information systems in the organization of production in transport: Author. dis. on sois. uch. step.* Transport and transport-technological systems of the country, its regions and cities, organization of production in transport.
4. Lakhno, V.A. (2009). Ensuring the security of automated information systems of transport enterprises in the context of the growth of transit traffic. *Book of Science Practitioners of the Viyskiy Institute of the Kiev National University for the Name of Taras Shevchenko*, (21), 110–120.
5. Karpeev, D.O., Ostapenko, G.A., Belonozhkin, V.I. (2006). Risk management strategies in socio-technical information systems. *Magazine "Information and Security,* (2), 133-134.
6. Information Security Management. Audit Check List for SANS Electronic resource. / Electron, text data. and count. dan. www.sans.org / score / checklists / ISO17799checklist.pdf
7. The concept of the state program for the development of motor transport until 2014. http://www.ei.com.ua/news/363368-ukraina-razrabotala-koncepciju-gosprogrammy-razvitija-avtotransporta-do.html
8. The concept of the development of the transport and road complex (TDK) of Ukraine until 2015 and the subsequent period. http://www.uts.in.ua/ru/kontseptsiya_rozvytku_transportno-dorozhnogo_kompleksu_tdk_ ukray iny _ do_ 2015_roku_i_podals.html
9. Susanto H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.
10. Eloff, J. H., & Eloff, M. (2003, September). Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130-136).
11. Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation-assets, threat and vulnerability. *Computer Standards & Interfaces*, *26*(6), 501-513.
12. Лахно, В. А. (2013). Проблеми інформаційної безпеки систем диспетчерського управління і збирання даних. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, (39), 168-175.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Valerii A. Lakhno
Dr. Tech. Sc., Professor, Head of the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Borys S. Husiev
Cand. Tech. Sc. (Ph.D), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-1658-7822
gusevbs@nubip.edu.ua

Victor V. Smolii
Cand. Tech. Sc. (Ph.D), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-2834-6989
dr.v.smoliy@gmail.com

Andrii I. Blozva
Cand. Pedag. Sc. (Ph.D.), Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Dmytro Y. Kasatkin
Cand. Pedag. Sc. (Ph.D.), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-2642-8908
d.kasatkin@nubip.edu.ua

Tetiana Y. Osypova
Cand. Pedag. Sc. (Ph.D), Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

METHODS OF SYSTEM ANALYSIS IN THE FORMATION OF INFORMATION SECURITY POLICY ON TRANSPORT

Abstract. Approaches to the application of methods of system analysis to solve problems related to information security of enterprises in transport, which have a complex IT structure with a large number of components. It is shown that the active expansion of the areas of informatization of the transport industry, especially in the segment of mobile, distributed and wireless technologies, is accompanied by the emergence of new threats to information security. It is shown that in order to build an effective information security system, the selection and implementation of adequate technical means of protection should be preceded by a stage of description, analysis and modeling of threats, vulnerabilities, followed by calculation of risks for IS and determining the optimal strategy for information security system. After evaluating the different NIB options according to several criteria, a decision is made: if the recommendations coincide, the optimal solution is chosen with greater confidence. If there is a contradiction of recommendations, the final decision is made taking into account its advantages and disadvantages, for example, the strategy of information security system development is chosen, which turned out to be optimal for at least two criteria. If different NIB development strategies are obtained for all three criteria, it is necessary to vary the values of pessimism-optimism in the Hurwitz criterion or change the data, for example, about possible threats to IP or automated enterprise management system. An algorithm for modeling the decision-making process for selecting the optimal strategy for managing investment design components of the information security system for the transport business entity is proposed.

Keywords: informational security; methods of system analysis; criterion for evaluating the information security system.

ISSN 2663 - 4023

REFERENCES

1. European Conference of Ministers of Transport (ECMT). http: // international transport forum.org/pub/pdf/06Europe-AsiaRU.pdf
2. Transport informatization: Best examples. http://www.cnews.ru/news/top/index.shtml?2013/02/11/518663
3. Volynskaya, A. V. (2004). *Increasing the stability of information systems in the organization of production in transport: Author. dis. on sois. uch. step.* Transport and transport-technological systems of the country, its regions and cities, organization of production in transport.
4. Lakhno, V.A. (2009). Ensuring the security of automated information systems of transport enterprises in the context of the growth of transit traffic. *Book of Science Practitioners of the Viyskiy Institute of the Kiev National University for the Name of Taras Shevchenko*, (21), 110–120.
5. Karpeev, D.O., Ostapenko, G.A., Belonozhkin, V.I. (2006). Risk management strategies in socio-technical information systems. *Magazine "Information and Security,* (2), 133-134.
6. Information Security Management. Audit Check List for SANS Electronic resource. / Electron, text data. and count. dan. www.sans.org / score / checklists / ISO17799checklist.pdf
7. The concept of the state program for the development of motor transport until 2014. http://www.ei.com.ua/news/363368-ukraina-razrabotala-koncepciju-gosprogrammy-razvitija-avtotransporta-do.html
8. The concept of the development of the transport and road complex (TDK) of Ukraine until 2015 and the subsequent period. http://www.uts.in.ua/ru/kontseptsiya_rozvytku_transportno-dorozhnogo_kompleksu_tdk_ ukray iny _ do_ 2015_roku_i_podals.html
9. Susanto H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.
10. Eloff, J. H., & Eloff, M. (2003, September). Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130-136).
11. Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation-assets, threat and vulnerability. *Computer Standards & Interfaces*, *26*(6), 501-513.
12. Lakhno, V. A. (2013). Problemy informatsiinoi bezpeky system dyspetcherskoho upravlinnia i zbyrannia danykh. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, (39), 168-175.