КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.135147
УДК 378.4:004.71:004.056

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

Смолій Віктор Вікторович
к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки 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, мереж та кібербезпеки 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, мереж та кібербезпеки 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, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Місюра Максим Дмитрович
к.т.н., доцент кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-9061-3462
mdm@nubip.edu.ua

МОДЕЛЬ АДАПТИВНОГО УПРАВЛІННЯ ПРАВАМИ ДОСТУПУ З ВИКОРИСТАННЯМ АПАРАТУ МЕРЕЖ ПЕТРІ

Анотація. У статті описано концептуальну модель адаптивного управління кіберзахистом інформаційно-освітнього середовища сучасного університету (ІОСУ). Мережі Петрі застосовано як математичний апарат для вирішення завдання адаптивного управління правами доступу користувачів ІОСУ. Запропоновано імітаційну модель та виконано моделювання у пакеті PIPE v4.3.0. Показано можливість автоматизації процедур коригування профілю користувача для мінімізації або нейтралізації кіберзагроз в ІОС. Запропоновано модель розподілу завдань користувача в комп'ютерних мережах ІОСУ. Модель, на відміну існуючих, побудована з урахуванням математичного апарату мереж Петрі і містить змінні, які дозволяють скоротити потужність простору станів. Доповнено метод контролю прав доступу (МКПД). Доповнення торкнулися аспектів перевірки прав доступу, які запитуються завданням та вимогами політики безпеки, ступенем узгодженості завдань та дозволених до доступу вузлів ІОСУ. Коригування правил та метрик безпеки для нових задач або перерозподілу задач описано в нотації мереж Петрі.

Ключові слова: інформаційно-освітнє середовище університету; кібербезпека; управління правами доступу; політика безпеки; математична модель; мережі Петрі; коригування правил.

ISSN 2663 - 4023

ВСТУП

Сучасний рівень застосування інформаційних технологій (ІТ) та систем (ІТС) в освіті досяг найвищого рівня. При цьому виник новий термін – інформаційно-освітнє середовище університету (ІОСУ) [1, 2]. Як і будь-який об'єкт інформатизації ІОСУ вимагає вирішення завдань захисту інформації та кібербезпеки (КрБ) [3,4]. При цьому більшість фахівців у галузі ІТ наголошують на необхідності першочергового пріоритету завдань збереження цілісності, конфіденційності та доступності інформації, незалежно від її функціонального призначення [5]. Загальним первинним завданням при побудові ефективних систем захисту та КрБ ІОСУ залишається обстеження конкретного об'єкта захисту, формування моделей потенційного порушника (комп'ютерного зловмисника – КЗЛ) та кіберзагроз [1–5]. Реалізація вищезгаданих кроків дозволить зрештою отримати адекватні вимоги до систем захисту інформації (СЗІ) ІОСУ.

В умовах ускладнення сценаріїв кібератак аналітикам служб інформаційної безпеки необхідно достатньо оперативно реагувати на кібератаки, аномалії, загрози. Це робить актуальним завдання пошуку нових способів підвищення результативності прийняття рішень у завданнях реагування на спроби деструктивного втручання з боку КЗЛ або несумлінного персоналу в роботу об'єктів інформатизації, у тому числі ІОСУ.

На думку багатьох фахівців, досить перспективним є можливість опису функціональних моделей різних систем захисту ІОСУ в термінах теорії мереж Петрі [4, 5, 7, 8]. Таке представлення дозволить аналітикам ІБ та ЗІ деталізувати кіберзагрози в ІОСУ. Окрім того, надалі, можливе визначення станів, які потенційно визначають вразливості ІОС перед новими кіберзагрозами. Також розглядається перспективність застосування даної моделі на основі мереж Петрі (і Петрі-Маркова) та розфарбованих мереж Петрі як математичної та алгоритмічної складових, що проектується інтелектуалізованою системою підтримки прийняття рішень (ІСППР) у процесі аналізу кіберзагроз для ІОСУ. На нашу думку, дані міркування роблять нашу роботу релевантною та підвищують результативність у процесі створення ІСППР у завданнях ЗІ та КрБ ІОСУ.

АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ ТА ПОСТАНОВКА ПРОБЛЕМИ ДОСЛІДЖЕНЬ

У роботах [3-5, 8, 9] були представлені результати досліджень з застосування мереж Петрі для опису моделі кіберзагроз. І хоча дані роботи зробили певний теоретичний внесок у даному питанні, на наш погляд, запропоновані авторами моделі дещо складно реалізувати програмними засобами, зокрема в ІСППР з ЗІ та КрБ ІОС.

Беручи за основу роботи [3] та [5] моделі загроз можна побудувати, використовуючи досить наочну табличну форму відображення загроз при актуалізації питання оцінки захищеності ІОСУ. Але, як було зазначено раніше, цей підхід до створення моделей загроз є трудомістким. Крім того, зростання кількості загроз робить подібний табличний формат подання складним для сприйняття, особливо фахівцям з невеликим досвідом роботи у сфері КрБ.

Мережі Петрі (і Петрі-Маркова) успішно використовувалися для опису моделей порушника [10, 11]. Однак автори не розглядали можливість коригування моделі порушника (КЗЛ) в ІОСУ, зокрема шляхом об'єднання її з моделями на основі теорії графів, що дозволило б більш точно описати переходи станів у процесі ймовірного подолання КЗЛ периметрів (меж) кіберзахисту ІОСУ.

У роботах [3, 8, 9] моделі СЗІ розглядалися як попередньо виділені в мережі Петрі послідовності елементарних операцій, з яких можлива кібератака. Моделі дозволяли прораховувати ймовірність реалізації різних атак за певний проміжок часу. Проте, розглянуті в [9, 10] моделі не дозволяли розрахувати характеристики часу в процесі реалізації нових кіберзагроз.

У роботах [5, 12] також пропонувалися моделі, засновані на мережах Петрі, що описують процеси реалізації загроз в інформаційних системах (ІС). Незважаючи на те, що зазначені моделі, дозволяли провести оцінку багатьох параметрів захищеності об'єктів, зокрема, ймовірності реалізації загроз, часу на реалізацію загроз, узгодженість дій КЗЛ, вони є не до кінця завершеними. Зокрема, у цих дослідженнях не розглянуто питання вирішення конфліктних ситуацій, що виникають при зміні станів ІС при перебігу атак, що належать до різних класів. Ця обставина, на наш погляд, обмежує практичну значення даних досліджень.

Таким чином, синтез нових моделей, а також доповнення існуючих моделей та методів адаптивного управління кіберзахистом ІОСУ з використанням можливостей апарату мереж Петрі та враховуючи потенціал візуалізації мереж Петрі, може стати ефективним інструментарієм для прогнозування стану захищеності ІОСУ та інших великих навчальних закладів. Це дозволить значно спростити розуміння нових кіберзагроз і надалі можливе результативне застосування пропонованих підходів аналітиками служб ЗІ, ІБ та КрБ різних об'єктів інформатизації.

МЕТА ТА ЗАВДАННЯ РОБОТИ

Мета – розвиток моделей та методів, що сприяють підвищенню стійкості функціонування комп'ютерних мереж університетів на основі адаптивного управління механізмами кібербезпеки в умовах збільшення кількості та складності деструктивних несанкціонованих впливів.

Для досягнення мети дослідження вирішуються *завдання* з розробки:

концептуальної моделі адаптивного управління кіберзахистом університету з використанням апарату мереж Петрі;

моделі розподілу завдань користувача в комп'ютерних мережах університетів;

доповнень до методу контролю прав доступу в контексті перевірки прав доступу, які виникають з завдань та вимог політики безпеки та ступеня узгодженості задачі та дозволених до доступу вузлів інформаційно-освітнього середовища університету.

МЕТОДИ ТА МОДЕЛІ

Відповідно до мети нашого дослідження в даному розділі статті описано концептуальну модель адаптивного управління кіберзахистом ІОСУ.

Розглянуто конкретний приклад вирішення завдання адаптивного управління правами доступу користувачів з використанням апарату мереж Петрі та відповідного програмного забезпечення, яке дозволяє автоматизувати коригування профілю користувача ІОС, а також за допомогою інтеграції модуля ІСППР рекомендувати способи нейтралізації кіберзагроз в ІОС.

Постановку завдань управління правами доступу сформулюємо так: 1) побудувати модель розмежування доступу для заданої ІОСУ; 2) визначити керовані

параметри моделі; 3) виконати параметризацію ризику порушення конфіденційності інформації для ІОСУ.

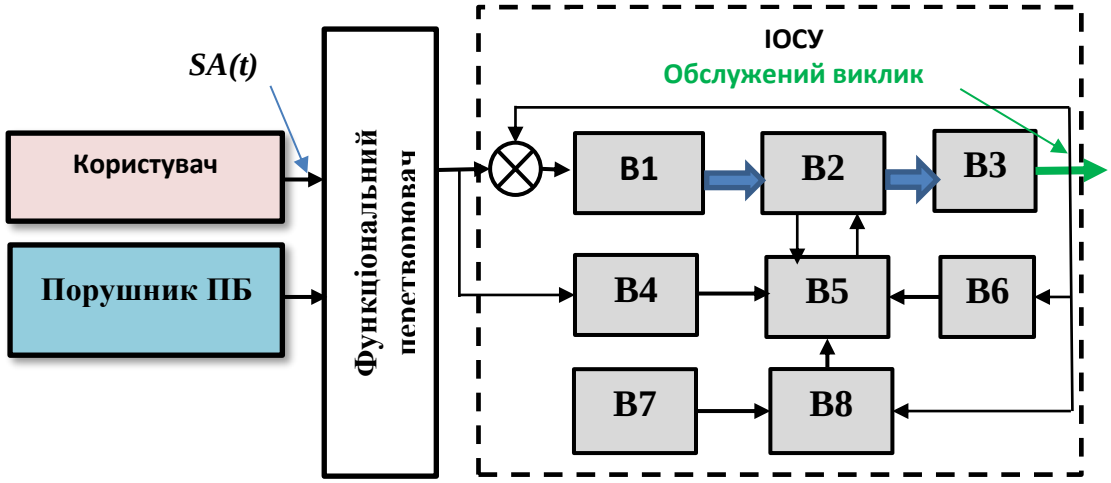

Рис. 1. Схема концептуальної моделі адаптивного управління кіберзахистом ІОСУ

Прийняті позначення: В1 – блок інформаційно-вимірювальних пристроїв в ОБІ; В2 - блок багатоканальних керуючих пристроїв; В3 - ОБІ як об'єкт управління доступом до ресурсів; В4 - блок прогнозування станів в ОБІ; В5 – блок прийняття рішень про право доступу; В6 – блок розрахунку ефективності за кількістю реалізованих загроз, пов'язаних із порушенням доступу до ОБІ; В7 – блок апріорної інформації; В8 – блок змінних моделей

Формальна математична постановка задачі оптимізації схеми розмежування доступу в ОБІ. Вихідні дані: 1) Об'єкти доступу в ОБІ - $AO = \{ao_i\}, i = \overline{1, I}$; 2) суб'єкти доступу в ОБІ - $SA = \{sa_j\}, j = \overline{1, J}$; 3) комунікаційні вузли (КВ) в ОБІ - $CN = \{cn_k\}, k = \overline{1, K}$; 4) адаптивний механізм, який дозволяє підтримувати метрики безпеки доступу в ОБІ на заданому рівні – $AM^0 = \{am^0_{i,j}\}, i = \overline{1, I}, \ j = \overline{1, J}$.

Вважатимемо, що прийнятний рівень захисту ОБІ досягнуто, якщо виконуються умови, описані в таблиці 1.

Таблиця 1

Умови, за яких досягнуто прийнятний рівень захисту ОБІ (*для завдання оптимізації управління доступом на ОБІ*) [з урахуванням 8, 9, 12]

№	Параметр	Умова
1	Адаптивний механізм, який дозволяє підтримувати метрики безпеки доступу в ОБІ на заданому рівні [5, 9].	$am_{i,j} = \begin{cases} 1, \text{ if } am_i \text{ it is placed on} \\ \text{a node } cm_k; \\ 0, \text{ Otherwise}. \end{cases}$

ISSN 2663 - 4023

2	Збитки від ймовірного несанкціонованого доступу до ресурсів - [8, 12].	*Дивись примітку*
3	Структури обчислювальної мережі ОБІ –	$ns_{m,n} = \begin{cases} 1, \text{ if } \left(cn_m \in NS_o\right) \& \left(cn_n \in NS_o\right); \\ 0, \text{ Otherwise}. \end{cases}$ $where \quad NS_o - \text{Network objects.}$
Керовані параметри (задаються адміністратором ЗІ та КрБ)		
1	Ознаки загального доступу до ресурсів ОБІ – $SV = \{sv_i\}$ [6, 9].	$sv_i = \begin{cases} 1, \text{ if the general access to} \\ \text{a node } sv_i \text{ is allowed}; \\ 0, \text{ Otherwise}. \end{cases}$
2	Розміщення на вузлах ОБІ – $MP^1 = \left[mp^1_{i,k}\right]$	$mp^1_{i,k} = \begin{cases} 1, \text{ if } ao_i \in cn_k; \\ 0, \text{ Otherwise}. \end{cases}$
3	Розміщення на вузлах ОБІ - $MP^2 = \left[mp^2_{j,k}\right]$.	$mp^2_{j,k} = \begin{cases} 1, \text{ if } sa_j \in cn_k; \\ 0, \text{ Otherwise}. \end{cases}$
Примітка **:** Збиток від можливого несанкціонованого доступу до ресурсів (рядок 2) визначимо степенем інформаційних ресурсів на вузлі ОБІ, а також профілем користувача (з урахуванням характеристик можливих порушників, див. таблицю 2).		

Умови, у яких досягнуто прийнятний рівень захисту ОБІ (*завдання оптимізації управління доступом на ОБІ*) розглядаються у сукупності з даними таблиці 2.

Вважатимемо, що цільовою функцією є величина ймовірного очікуваного збитку від несанкціонованого доступу до інформаційних ресурсів (ІР) ОБІ (далі ІР ОБІ).

Таблиця 2

Характеристики можливих порушників [9, 10, 13]

Класифікація	Характеристика
За мотивами порушення	Порушення цілісності, конфіденційності, доступності з корисливою чи іншою метою.
За рівнем поінформованості та кваліфікації КЗЛ	Порушник (чи КЗЛ): 1) високий рівень знань; 2) достатні знання для збору інформації, застосування відомих експлойтів та написання власного програмного забезпечення для здійснення кібератаки; 3) КЗЛ не є авторизованим користувачем ОБІ.
За місцем дії	Без безпосереднього (фізичного) доступу на територію ОБІ. Порушник діє віддалено, наприклад, через мережі загального користування.

ISSN 2663 - 4023

Цей параметр визначається як міра розбіжності між реальним та оптимальним розмежуванням доступу користувачів до ІР для конкретного ОБІ.

$$TF = \sum_{i=1}^{I}\sum_{j=1}^{J} da_{i,j}^{0} \cdot \left| am_{i,j} - am_{i,j}^{0} \right|, \quad (1)$$

де $\{am_{i,j}\}$ – елементи множини, що відображають вже реалізовані права доступу.

Вважаємо, що

$$am_{i,j} = \sum_{k=1}^{K} ns_{i,k} \cdot w_{k,j}^{0}; \quad (2)$$

$$w_{k,j}^{0} = w_{k,j}^{1} + sv_i \cdot \left(1 - w_{k,j}^{1}\right); \quad (3)$$

$$w_{k,j}^{1} = \sum_{k=1}^{K} \left(mp_{i,k}^{2} \cdot mp_{k,j}^{1} \right). \quad (4)$$

Таким чином, отримано формулювання завдання розмежування прав доступу. Дане завдання відноситься до завдань нелінійної оптимізації вектору керованих параметрів у булевих змінних:

$$UD = \min \sum_{i-1}^{I}\sum_{j=1}^{J} da_{i,j}^{0} \cdot \left| am_{i,j} - am_{i,j}^{0} \right| \quad (5)$$

для наступних обмежень

$$\sum_{k-1}^{K} da_{i,j}^{1} \le 1 \quad (6)$$

та $$\sum_{k-1}^{K} da_{i,j}^{2} \le 1. \quad (7)$$

Постійне коригування профілю активного користувача передбачало застосування спеціального ітераційного алгоритму [14]. Цей алгоритм базується на неявному зворотному зв'язку сервера з користувачем ресурсами конкретного ОБІ. Ключовим фактором є статистика запитів. Оцінювання поточного профілю користувача застосовувалася для того, щоб рангувати користувачів на групи за ступенем небезпеки для ІР ОБІ. Прийнято: а) користувач; б) потенційно небезпечний користувач; в) небезпечний користувач; г) порушник.

Оптимізація налаштувань процедур управління доступом здійснювалася на основі визначення таких параметрів: 1) Інтенсивність переходів $\lambda_{i,j}(t)$ (визначені на основі регресійних моделей) [14]; 2) параметризація ризику, пов'язаного з порушенням конфіденційності інформації в ОБІ. Визначається як багатофакторна регресійна модель 2-го порядку [15]:

$$P_r(\tau) = da_0 + \sum_{k=1}^{m} da_k \cdot h_k + \sum_{ao=1}^{m} da_{ao,ao} \cdot h_{ao}^{2} + \sum_{i,j=1}^{m} da_{i,j} \cdot h_i \cdot h_j, \; i \ne j,$$

де $h = (h_1, ..., h_m)^T$ – керовані параметри, що регламентують правила, що розмежовують доступ у мережах конкретних ОБІ: τ – час.

Відносно будь-якого ОБІ з розподіленою схемою доступу до ресурсів, модель абонентських завдань визначена так

$$\sum = (PN, PIS, AT, s_0, FTR, MRT, RES), \quad (8)$$

де $PN = (TGR, T, MPN, F)$ – ІР ОБІ (представлені мережею Петрі); $TGR = \{tgr\}$ – множина вершин графа (вершина – постачальник ІР ОБІ); $T = \{t\}$ – число переходів між вершинами; $MPN = (mpn_1, ..., mpn_n)$ – розмітка мережі Петрі; F - відношення сусідства вершин; PIS – політики інформаційної безпеки; AT - активні завдання, ініційовані користувачами ІР ОБІ; s_0 – початковий стан $S = \{s\}$; $FTR: PN \times AT \times MRT \times PIS \times A \to S$ – функція переходу між станами ІР ОБІ; $MRT = \langle CL, U \rangle$ – маркери в мережі Петрі, CL – клас ресурсів, які запитують абоненти (користувачі) (U); RES – поточна позиція у правах доступу до ІР в ОБІ.

З урахуванням попередніх міркувань, отримані такі правила для програмного продукту «Аналізатор загроз» (детально описаний у [14]) для прийняття рішення щодо можливості доступу абонента (користувача до ІР):

абоненту U (користувачу ІР ОБІ) санкціоновано доступ до ІР власника OWR, якщо процедура взаємної автентифікації відбулася коректно. Для власника ІР OWR визначається локальний обліковий запис. При цьому в даному записі відображені усі абоненти та їх тип доступу відповідно до ПБ:

$$Has\ COMP\ Ass\ Ri(U, OWR, PIS) = \begin{pmatrix} Is\ TRU\ By\ U(U, OWR) \wedge Is\ TRU\ By\ TGR(OWR, U) \wedge \\ (MapU\ To\ UD(OWR, U) \neq 0) \end{pmatrix} \wedge \quad (9)$$
$$Is\ Acc\ AL\ By\ PIS(U, OWR, PIS),$$

по відношенню до ІР ОБІ, локальні облікові записи на вузлах, у яких відображені абоненти, повинні також мати право доступу – RI до об'єкту Ob :

$$Has\ FC\ Ass\ Ri(U, OWR, PIS, Ob, RI) = \begin{pmatrix} Is\ TRU\ By\ U(U, OWR) \wedge \\ \wedge\ Is\ TRU\ By\ TGR(OWR, U) \wedge \\ (ListU = MapU\ To\ UD(OWR, U) \neq 0) \end{pmatrix} \wedge \quad (10)$$
$$Is\ Acc\ AL\ By\ PIS(U, OWR, PIS),$$

де Acc – доступ; RI – право доступу до ІР; AL – дозволено; TRU – є надійним; $MapU$ – картка абонента/користувача; $ListU$ – локальний обліковий запис абонента; $MapU\ To\ UD$ – функція, яка відображає множину користувачів ІР в ОБІ у форматі локальних облікових записів власника ІР – OWR .

Беручи до уваги роботи [5, 9, 12, 13] були запропоновані уточнення до методу контролю і управління доступом (КУД), з урахуванням специфіки мережі ОБІР. Уточнений і доповнений метод КУД полягає в перевірці прав доступу, які запитуються завданням та вимогами політики безпеки, окрім того, узгодженням задачі і дозволених для доступу вузлів ОБІ. Для вузлів ОБІ, є також процедура перевірки прав доступу для всіх абонентів, які мають відповідні права. В результаті буде отримано безліч вузлів, на яких абонентські завдання можуть бути виконані. При цьому враховуються поточні показники політики безпеки для конкретного ОБІ і метрики безпеки. Можливе коригування правил для нових завдань або перерозподілених завдань. Ці коригування або перерозподіл завдань можуть бути описані в нотації мереж Петрі з урахуванням математичної моделі, яка описується виразами (8) - (10).

ISSN 2663 - 4023

ЕКСПЕРИМЕНТ

Спираючись на наведені вище міркування, в базисі модифікованих мереж Петрі (ММП) була розроблена модель адаптивного рольового управління доступом до ресурсів ОБІ (Система управління доступом – СУД). Виконано імітаційне моделювання у пакеті PIPE v4.3.0 (Platform Independent Petri net Editor). Такий підхід дозволив коректно описати конфліктні ситуації, окрім того, була врахована особливість обробки запитів, які виникають у більшості ІС ОБІ в процесі багатокористувацького режиму роботи. На рис. 2 показано схему імітаційної моделі. Схема відображає логічну структуру операційної моделі системи прав доступу (для варіанта триступінчастого управління). Позиції та переходи у мережевій моделі в базисі ММП показані в таблиці 3.

У процесі досліджень було виконано оцінку результативності запропонованих моделей та уточнень до методу контролю прав доступу. Для оцінки результативності запропонованих рішень, використовувався показник, що характеризує скорочення витрат часу на прийняття рішень. Відповідно, оцінювалися витрати часу на обробку даних до та після застосування, запропонованих моделей та методу. Імітаційний експеримент проведено для 400 обчислювальних вузлів. Кожному вузлу поставлено у відповідність віртуальна машина. Кількість реалізованих кіберзагроз, до імплементації в інтегровану систему ІБ та КрБ ОБІ та після її впровадження, показано на рис. 3.

Таблиця 3

Позиції та переходи до мережевої моделі системи правами доступу у базисі модернізованих мереж Петрі

Позиції	
Позначення	Опис позиції для користувача
*P*1	активний стан
*P*2	користувач допущений до роботи в проекті
*P*3	допущений до роботи з функціональними компонентами
*P*4	допущений до файлів інформаційних ресурсів ОБІ
*P*5	перевірка прав для завдання
*P*6	перевірка прав доступу до функціональних компонентів
*P*7	перевірка прав доступу до файлів
*P*8	відновлення вихідного стану СУД
*P*9	обмеження активності в часі (наприклад, під час коригування завдання)
Переходи	
Позначення	Опис
T*1*…T*8*	відображають сукупність умов переходу (і модифікації) маркерів з однієї позиції мережі до інших. Умови визначені набором апріорних даних

ISSN 2663 - 4023

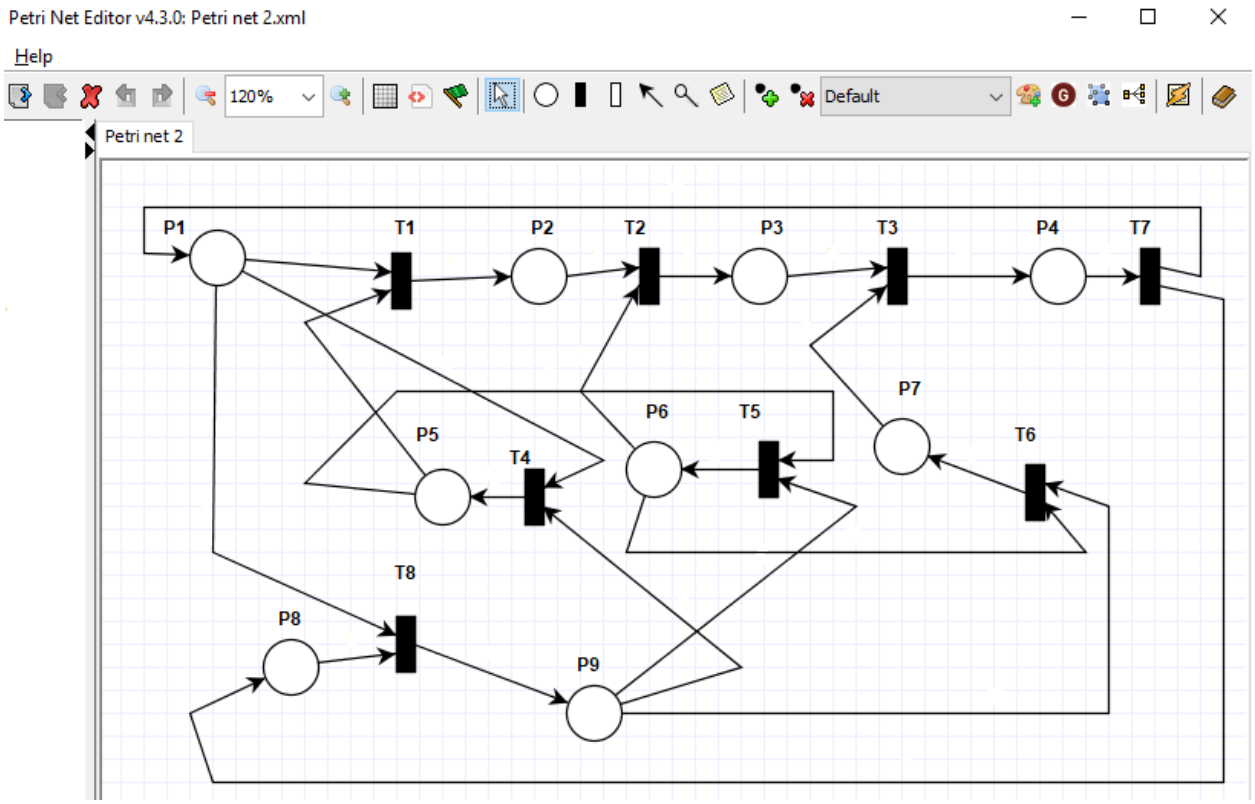

Рис. 2. Схема імітаційної моделі адаптивного управління правами доступу з урахуванням рольового регулювання

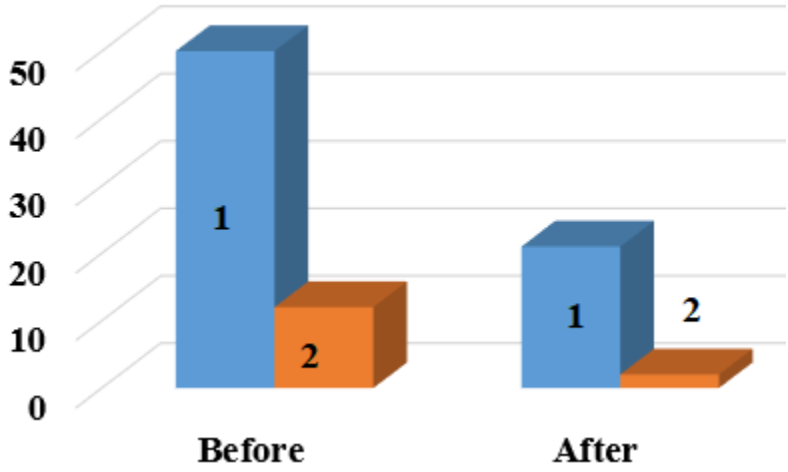

Рис. 3. Оцінка інформаційної безпеки ОБІ

1- Загальна кількість кіберзагроз, які були реалізовані в ОБІ; 2- Кіберзагрози, пов'язані з порушенням прав доступу та перевищенням повноважень

Отримані в ході імітаційного моделювання статистичні дані дали підставу встановити конкретні характеристики СУД для компаній, що брали участь в апробації моделі.

ОБГОВОРЕННЯ

До переваг нашого дослідження можна віднести той факт, що запропоновані рішення, зокрема, розроблена концептуальна модель адаптивного управління правами доступу з використанням апарату мереж Петрі, а також моделі та метод, були успішно апробовані в підсистемі адміністрування інформаційної та кібербезпеки кількох великих університетів України, а також у комерційних підприємствах м. Києва та Дніпро. Створені на основі запропонованих рішень програмні продукти дозволили автоматизувати контроль, супровід та зміну облікових записів абонентів мереж ОБІ. При цьому, у програмних продуктах (зокрема система «Аналізатор загроз [14])» було закладено можливість коригувати рівні доступу абонентів до інформаційних ресурсів.

Певним недоліком у роботі, є невеликий ступінь апробації запропонованих рішень, тому що дослідження та робота в обраному напрямку триває.

Перспектива подальших досліджень визначається можливостями застосування отриманих результатів для подальшої алгоритмізації процесів, пов'язаних з аналізом ІБ та КрБ різних ОБІ, зокрема, для вирішення прикладних завдань, пов'язаних із проблематикою управління та контролю доступу в критично важливих комп'ютерних системах та об'єктах інформатизації. У цьому контексті наша робота продовжує попередні публікації авторів [14, 15].

ВИСНОВОК

У роботі отримано такі результати:

описано концептуальну модель адаптивного управління кіберзахистом об'єкта інформатизації (ОБІ). Розглянуто приклад вирішення задачі адаптивного управління правами доступу користувачів з використанням апарату мереж Петрі. Реалізовано відповідну модель та виконано імітаційне моделювання у пакеті PIPE v4.3.0. Показано можливість автоматизації процедур коригування профілю користувача для мінімізації або нейтралізації кіберзагроз в ОБІ;

описано модель розподілу завдань, призначених користувачами, у комп'ютерних мережах об'єктів інформатизації. Базою моделі послужив математичний апарат мереж Петрі. На відміну від існуючих, модель містить змінні, які дозволяють зменшити потужність підпростору станів. Також підвищилась результативність моделювання, зокрема, за рахунок скорочення витрат часу на прийняття рішень, пов'язаних із регламентацією прав доступу;

уточнено та доповнено метод контролю прав доступу (МКПД). Уточнення торкнулися аспектів перевірки прав доступу, які випливають з завдань та вимог політики безпеки. Крім того, враховувалася узгодженість завдання та дозволених до доступу вузлів ОБІ. Для вузлів ОБІ також розглянуто процедуру перевірки прав доступу абонентів, які мають відповідні права. Модель враховує поточні показники політики безпеки для конкретних ОБІ та метрики безпеки з можливим коригуванням останніх. Коригування правил та метрик безпеки для нових завдань або перерозподілених задач описано в нотації мереж Петрі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Буйницька, О. П., Грицеляк, Б. І. (2013). Студент в інформаційно-освітньому середовищі сучасного університету. *Інформаційні технології і засоби навчання*, *36*(4), 66-83.

2 Ворожбит, А. В. (2018). Веб-орієнтоване інформаційно-освітнє середовище закладу освіти. *Інформаційні технології в освіті*, (3), 20-29.

3 Кидираліна, Л. М., Ахметов, Б. С., Лахно, В. А. Моделювання процедури прийняття рішень щодо фінансування засобів кібербезпеки інформаційно-освітнього середовища університету. *Захист інформації*, *20*(2), 120-127.

4 Liu, X., Zhang, J., Zhu, P. (2017). Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory. *International Journal of Critical Infrastructure Protection*, (16), 13–25.

5 Супруненко, О. О. (2010). Модифікація підсистем захисту інформації на основі мереж Петрі. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення у сучасних технологіях*, (57), 173-177.

6 Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. *Eastern-European Journal of Eenterprise Technologies*, *1*(2), 4–15.

7 Дудикевич, В. Б., Гарасим, Ю. Р., Нечипор, В. В. (2011). Методи моделювання систем захисту інформації для корпоративних мереж зв'язку. *Сучасний захист інформації*, (4), 54-60.

8 Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D., & Fernando, A. (2016, January). Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In Consumer Electronics (ICCE), 2016 IEEE International Conference on (pp. 502–503). IEEE.

9 de Carvalho, M. A., Bandiera-Paiva, P. (2017, October). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling. In Security Technology (ICCST), 2017 International Carnahan Conference on (pp. 1–8). IEEE.

10 Appel, M., Konigorski, U., Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri Nets. IFAC-PapersOnLine, *51*(2), 254–259.

11 Gao, Z., Zhao, C., Shang, C., Tan, C. (2017, October). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), 2017 (pp. 78–83). IEEE.

12 Narayanan, M., Cherukuri, A. K. (2018). Verification of Cloud Based Information Integration Architecture using Colored Petri Nets. *International Journal of Computer Network and Information Security*, *10*(2), 1.

13 Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. *Eastern-European Journal of Enterprise Technologies*, *6*(9 (84)), 32–44. https://doi.org/10.15587/1729-4061.2016.85600.

14 Beketova, G., Akhmetov, B., Korchenko, A., Lakhno, V., Tereshuk, A. (2017). Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition. *Computer modelling and new technologies*, *21*(2), 7–16.

15 Lakhno, V., Petrov, A., & Petrov, A. (2017). Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport. У *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017* (с. 113–127). Springer International Publishing. https://doi.org/10.1007/978-3-319-67229-8_11

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

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

Victor V. Smolii
Cand. Tech. Sc. (Ph.D), Docent, Associate Professor at the Department of Computer System, Networks and Cybersecurity
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, Networks and Cybersecurity
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, Networks and Cybersecurity
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, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Maksym D. Misiura
Cand. Tech. Sc. (Ph.D), Associate Professor at the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9061-3462
mdm@nubip.edu.ua

MODEL OF ADAPTIVE ACCESS RIGHTS MANAGEMENT USING PETRI NETS

Abstract. The article describes the conceptual model of adaptive management of cybersecurity of the information and educational environment of a modern university (IOSU). Petri nets are used as a mathematical apparatus to solve the problem of adaptive management of access rights of IOS users. A simulation model is proposed and modeling in PIPE v4.3.0 package is performed. The possibility of automating the procedures of user profile adjustment to minimize or neutralize cyber threats in IOS is shown. The model of distribution of tasks of the user in computer networks of IOSU is offered. The model, in contrast to the existing ones, is based on the mathematical apparatus of Petri nets and contains variables that reduce the power of the state space. The method of access control (ICPD) has been supplemented. The additions addressed aspects of the verification of access rights, which are required by the tasks and requirements of the security policy, the degree of coherence of tasks and allowed access to the IOSU nodes. Adjusting security rules and metrics for new tasks or reallocating tasks is described in Petri net notation.

Key words: university information and educational environment, cybersecurity, access rights management, security policy, mathematical model, Petri nets, rule adjustment.

REFERENCES

1. Buinytska, O. P., Hrytseliak, B. I. (2013). Student v informatsiino-osvitnomu seredovyshchi suchasnoho universytetu. Informatsiini tekhnolohii i zasoby navchannia, *36*(4), 66-83.
2. Vorozhbyt, A. V. (2018). Veb-oriientovane informatsiino-osvitnie seredovyshche zakladu osvity. Informatsiini tekhnolohii v osviti, (3), 20-29.
3. Kydyralina, L. M., Akhmetov, B. S., Lakhno, V. A. Modeliuvannia protsedury pryiniattia rishen shchodo finansuvannia zasobiv kiberbezpeky informatsiino-osvitnoho seredovyshcha universytetu. Zakhyst informatsii, *20*(2), 120-127.
4. Liu, X., Zhang, J., Zhu, P. (2017). Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory. *International Journal of Critical Infrastructure Protection*, (16), 13–25.
5. Suprunenko, O. O. (2010). Modyfikatsiia pidsystem zakhystu informatsii na osnovi merezh Petri. Visnyk Natsionalnoho tekhnichnoho universytetu «KhPI». Seriia: Novi rishennia u suchasnykh tekhnolohiiakh, (57), 173-177.
6. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. *Eastern-European Journal of Eenterprise Technologies*, *1*(2), 4–15.
7. Dudykevych, V. B., Harasym, Yu. R., Nechypor, V. V. (2011). Metody modeliuvannia system zakhystu informatsii dlia korporatyvnykh merezh zviazku. *Suchasnyi zakhyst informatsii*, (4), 54-60.
8. Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D., & Fernando, A. (2016, January). Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In Consumer Electronics (ICCE), 2016 IEEE International Conference on (pp. 502–503). IEEE.
9. de Carvalho, M. A., Bandiera-Paiva, P. (2017, October). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling. In Security Technology (ICCST), 2017 International Carnahan Conference on (pp. 1–8). IEEE.
10. Appel, M., Konigorski, U., Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri Nets. IFAC-PapersOnLine, *51*(2), 254–259.
11. Gao, Z., Zhao, C., Shang, C., Tan, C. (2017, October). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), 2017 (pp. 78–83). IEEE.
12. Narayanan, M., Cherukuri, A. K. (2018). Verification of Cloud Based Information Integration Architecture using Colored Petri Nets. *International Journal of Computer Network and Information Security*, *10*(2), 1.
13. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. *Eastern-European Journal of Enterprise Technologies*, *6*(9 (84)), 32–44. https://doi.org/10.15587/1729-4061.2016.85600.
14. Beketova, G., Akhmetov, B., Korchenko, A., Lakhno, V., Tereshuk, A. (2017). Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition. *Computer modelling and new technologies*, *21*(2), 7–16.
15. Lakhno, V., Petrov, A., & Petrov, A. (2017). Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport. У *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017* (с. 113–127). Springer International Publishing. https://doi.org/10.1007/978-3-319-67229-8_11