КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.841
УДК 004.056.55:681.3.06

Гнатюк Сергій Олександрович
д.т.н., проф., проректор з наукових досліджень та трансферу технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@kai.edu.ua

Сидоренко Вікторія Миколаївна
к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Скуратівський Анатолій Анатолійович
аспірант
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0009-0000-0566-2394
a.skurativskyi@gmail.com

МОДЕЛЬ УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. У сучасному світі цифрових технологій питання забезпечення кібербезпеки набувають ключового значення при впровадженні ПЗ у різних сферах діяльності. Зростаюча складність систем, динамічність загроз та обмеженість ресурсів вимагають від розробників і замовників ПЗ ефективних механізмів управління вимогами кібербезпеки. У статті представлено інтегровану математичну модель управління вимогами кібербезпеки при впровадженні програмного забезпечення. Актуальність проблеми зумовлена зростанням складності сучасних інформаційних систем, необхідністю дотримання міжнародних стандартів безпеки та обмеженням ресурсів у процесі реалізації проєктів. Запропонована модель поєднує низку математичних методів, зокрема метод аналізу ієрархій (AHP), нечітку логіку, Байєсові мережі та математичне програмування, що забезпечує системний підхід до прийняття рішень. Розроблена авторами модель дозволяє визначати пріоритетність вимог, оцінювати їх відповідність за умов невизначеності, моделювати ризики та оптимально розподіляти ресурси з урахуванням обмежень бюджету та цілей безпеки. Експериментальне дослідження, проведене на основі стандарту NIST 800-53, підтвердило ефективність запропонованого підходу у зменшенні ризиків без перевищення доступних ресурсів. Результати роботи мають практичне значення для організацій, що впроваджують програмне забезпечення, орієнтуючись на сучасні вимоги кібербезпеки. Подальші дослідження будуть спрямовані на оптимізацію моделі, її практичну реалізацію для інших міжнародних стандартів.

Ключові слова: модель управління; кібербезпека; управління вимогами; моделювання ризиків; оцінка ризиків; пріоритезація вимог; програмне забезпечення; нечітка логіка; Байєсова мережа; математичне програмування; оптимізація ресурсів; міжнародні стандарти; стандарти кібербезпеки.

ВСТУП

З розвитком цифрових технологій питання забезпечення кібербезпеки набувають ключового значення при впровадженні програмного забезпечення (ПЗ) у різних сферах діяльності. Зростаюча складність систем, динамічність загроз та обмеженість ресурсів вимагають від розробників і замовників ПЗ ефективних механізмів управління вимогами кібербезпеки. Особливу актуальність це питання має в контексті дотримання

міжнародних стандартів, які визначають вимоги до системного забезпечення захисту інформації та надають організаціям чіткі вказівки щодо забезпечення належного рівня безпеки. Проте ці стандарти часто не передбачають практичних механізмів адаптації до конкретних умов проекту, особливо за обмежених фінансових і часових ресурсів. Попри наявність окремих підходів до оцінки ризиків, пріоритезації вимог або розподілу ресурсів, наразі є відсутні інтегровані моделі, здатні враховувати всі ці аспекти одночасно в умовах невизначеності та багатофакторності.

Постановка проблеми. У сучасних умовах кібербезпека стала однією з ключових вимог до ПЗ, особливо в критичних інфраструктурах, державному секторі та великих корпоративних системах. Під час впровадження ПЗ виникає потреба у врахуванні численних вимог безпеки, які регламентуються міжнародними стандартами, зокрема NIST 800-53, ISO 22316, MITRE ATT&CK тощо. Ці стандарти містять вичерпний перелік контрольних заходів, однак не передбачають єдиної системи для оцінки їхньої пріоритетності, взаємозв'язків чи адаптації до конкретних проєктів з обмеженим бюджетом та ресурсами. Внаслідок цього в реальних умовах часто відбувається вибір наосліп або недостатньо обґрунтоване виділення ресурсів на реалізацію певних вимог, що може призводити до зростання ризиків.

Крім цього, проблема ускладнюється багатофакторністю, невизначеністю вихідних даних та ймовірнісною природою ризиків. Класичні методи управління вимогами, як правило, не здатні ефективно обробляти нечітку інформацію або враховувати складні залежності між вимогами. В умовах постійної еволюції кіберзагроз необхідно мати адаптивний і формалізований інструмент, який дозволяє оперативно оцінювати ризики, формувати пріоритети, а також враховувати ресурсні обмеження. Існує потреба у впровадженні математичних моделей, здатних поєднувати методи пріоритезації, ймовірнісного аналізу, нечіткої логіки та оптимізації.

У контексті вищезазначеного особливо актуальним є створення цілісної інтегрованої моделі управління вимогами кібербезпеки, яка б відповідала сучасним викликам та міжнародним стандартам. Така модель має враховувати не лише формальні вимоги стандартів, а й специфіку конкретного проєкту, поточні ризики, доступні ресурси та можливість їх оптимального розподілу. Для цього необхідно провести аналіз математичних підходів та інструментів, які дозволяють вирішувати різні завдання в управлінні вимогами кібербезпеки — від формування залежностей і пріоритетів до моделювання ризиків і оптимізації рішень. Отже, **метою даної статті** є розробка та експериментальне дослідження моделі управління вимогами кібербезпеки при впровадженні ПЗ.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Для побудови моделі управління вимогами кібербезпеки при впровадженні ПЗ доцільно використовувати кілька математичних підходів та інструментів, кожен з яких дозволяє вирішувати різні завдання в управлінні вимогами кібербезпеки. Ось основні математичні методи, які можна застосувати [1] – [12]:

1) Логіка і теорія множин

- *Булева логіка:* Використовується для визначення відповідності між вимогами кібербезпеки та їхніми залежностями. Застосовується для опису умов або перевірки виконання вимог через логічні вирази та оператори [1].
- *Теорія множин:* Допомагає класифікувати та групувати вимоги кібербезпеки, аналізувати їх перетини, взаємозалежності та суперечності

між вимогами. Наприклад, множини вимог можуть бути розбиті на обов'язкові, рекомендовані та додаткові [2].

2) Моделювання з використанням графів та мереж

- *Графи залежностей:* Для побудови моделі вимог можна використовувати графи, де вершини представляють окремі вимоги, а ребра — залежності між ними. Це дозволяє візуалізувати взаємозалежність вимог і визначити критичні шляхи [3].
- *Петля Петрі:* Використовується для моделювання та аналізу послідовності та умов виконання вимог. Петлі Петрі дозволяють формалізувати процес управління вимогами, особливо коли існує багато паралельних процесів або залежностей між вимогами [4].

3) Теорія нечіткої логіки

- *Нечітка логіка (Fuzzy Logic):* Часто застосовується для оцінки виконання вимог, коли критерії виконання вимоги не є чітко визначеними або мають ступінь невизначеності. Це дозволяє моделювати рівень відповідності вимогам за допомогою нечітких множин і функцій належності [5].
- *Нечіткі правила та висновки:* Використовуються для прийняття рішень щодо пріоритезації вимог або оцінки рівня ризику з урахуванням можливих невизначеностей [5].

4) Ймовірнісні моделі та теорія ризиків

- *Байєсові мережі:* Можуть бути використані для моделювання ризиків, пов'язаних з вимогами кібербезпеки, враховуючи ймовірності виникнення певних загроз і їх вплив на вимоги. Байєсові мережі дозволяють визначити ймовірність невиконання вимог у залежності від певних умов [6].
- *Теорія ігор:* Застосовується для моделювання поведінки атакуючих та системи захисту, враховуючи можливі стратегії атак. Модель може бути корисною для прийняття рішень щодо пріоритетів вимог з точки зору кібербезпеки [7].

5) Математичне програмування та оптимізація

- *Цільова функція та обмеження:* Управління вимогами кібербезпеки часто потребує оптимізації обмежених ресурсів (часу, бюджету, людських ресурсів), тому корисно застосувати лінійне або нелінійне програмування для оптимізації виконання вимог [8].
- *Метаевристичні алгоритми (генетичні алгоритми, алгоритми рою):* Дозволяють розв'язувати завдання з пошуку оптимального набору вимог або визначення пріоритетів для виконання з урахуванням обмежень [9].

6) Теорія систем масового обслуговування

- *Моделі обслуговування запитів:* Може використовуватися для побудови моделей обробки вимог у процесі розробки ПЗ. Наприклад, застосування теорії черг допоможе визначити, скільки ресурсів і часу знадобиться для впровадження кожної вимоги з кібербезпеки [10].

7) Динамічне моделювання та симуляції

- *Моделі Монте-Карло:* Для оцінки можливого впливу різних ризиків на виконання вимог, особливо коли вимоги є ресурсозатратними або ризики змінюються з часом [11].
- *Агентно-орієнтоване моделювання:* Використовується для моделювання взаємодії між учасниками процесу впровадження вимог кібербезпеки, зокрема для моделювання поведінки атакуючих.

8) Аналіз ієрархій та методу аналізу ієрархій (AHP)

– *Метод AHP:* Застосовується для встановлення пріоритетів серед вимог кібербезпеки на основі їхньої важливості. Цей метод допомагає систематично зважувати та порівнювати різні вимоги, що особливо корисно при обмежених ресурсах [12].

У наступному розділі статті розглянуті методи будуть використовуватись для розроблення математичної моделі управління вимогами кібербезпеки при впровадженні ПЗ.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ МОДЕЛІ

Математична модель управління вимогами кібербезпеки при впровадженні ПЗ на основі міжнародних стандартів NIST, відповідно до [15], реалізується за допомогою наступних кроків:

Крок 1: Створення графу залежностей вимог

Нехай $G = (V, E)$ — орієнтований граф, де:

$V = \{v_1, v_2, ..., v_n,\}$ — множина вершин, кожна з яких представляє конкретну вимогу кібербезпеки R_i.

E Í $V' V$ — множина орієнтованих ребер, кожне з яких позначає залежність між двома вимогами.

Кожна вимога v_i має атрибути:

Важливість W_i — наскільки вимога критична для кібербезпеки системи.

Ризик R_i — ймовірність компрометації безпеки, якщо вимога не виконана.

Крок 2: Використання методу AHP для пріоритезації вимог

Використовуємо метод AHP для пріоритезації вимог на основі критеріїв важливості W_i і ризику R_i.

1) Створення матриці парних порівнянь для кожного критерію: Для вимог v_i і v_j, заповнюємо матриці парних порівнянь A_w (за важливістю) і A_R (за ризиком), де a_{ij} вказує, наскільки важлива вимога v_i порівняно з вимогою v_j за певним критерієм.

2) Визначення ваги вимог:

Обчислюємо власні вектори W і R для матриць A_w і A_R відповідно, які відображають ваги (або пріоритети) кожної вимоги за кожним критерієм.

Отримана векторна оцінка P вимог розраховується як:

$$P = aW + bR, \quad (1)$$

де a і b — коефіцієнти важливості критеріїв (визначаються експертно).

Крок 3: Застосування нечіткої логіки для оцінки рівня відповідності вимогам

Враховуємо, що деякі вимоги можуть мати нечітку відповідність. Наприклад, відповідність кожної вимоги v_i можна оцінювати за допомогою нечітких множин на основі лінгвістичних змінних:

Нечіткі змінні: «висока відповідність», «середня відповідність», «низька відповідність».

Функції належності $m_i(x)$ для кожної змінної нечіткої відповідності, де x Î $[0,1]$ — рівень відповідності вимоги v_i.

Оцінка відповідності кожної вимоги v_i обчислюється як:

$$Score(v_i) = max\{m_{висока}(x), m_{середня}(x), m_{низька}(x)\}. \quad (2)$$

Агрегація оцінок для визначення загального рівня відповідності всієї системи вимог, враховуючи середньозважені оцінки.

Крок 4: Моделювання ризиків за допомогою Байєсової мережі

Створюємо Байєсову мережу для моделювання впливу загроз на виконання вимог кібербезпеки.

1) Вузли мережі:

кожна вимога v_i стає вузлом, з атрибутом ризику R_i.

Додаткові вузли — потенційні загрози, що можуть впливати на виконання вимог.

2) Ймовірності вузлів:

Ймовірності компрометації вимоги $P(v_i | T_j)$, де T_j — загроза, яка впливає на вимогу v_i.

3) Розрахунок ризику системи: Використовуючи Байєсову мережу, можна обчислити ймовірність ризиків для кожної вимоги за умов присутності різних загроз.

4) Обчислення ризику для кожної вимоги з урахуванням відповідності:

$$Risk(v_i) = R_i \cdot Score(v_i). \quad (3)$$

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Визначаємо оптимальний розподіл ресурсів для реалізації вимог кібербезпеки з урахуванням [14] та пріоритетів і ризиків.

1) змінні:

x_i — частка ресурсів, виділена для вимоги v_i, де $0 \le x_i \le 1$;

2) цільова функція: мінімізуємо ризики невиконання вимог з урахуванням обмежених ресурсів:

$$min \sum_{i=1}^{n} (1 - x_i) \cdot Risk(v_i), \quad (4)$$

3) обмеження:

– обмеження на загальний бюджет:

$$\sum_{i=1}^{n} x_i \cdot C_i \le B, \quad (5)$$

де C_i — вартість виконання вимоги v_i, B — загальний бюджет.

– пріоритетність вимог: $x_i \ge p_i$ для всіх вимог v_i з високим пріоритетом, де p_i — мінімальний рівень виконання для пріоритетних вимог.

4) Вихідний розподіл ресурсів: розв'язавши оптимізаційну задачу, отримуємо оптимальні значення x_i для кожної вимоги v_i, які забезпечують мінімізацію ризиків при обмежених ресурсах.

Таким чином, було розроблено модель, яка дозволяє: визначити пріоритети серед вимог кібербезпеки (кроки 1–2); врахувати невизначеності та ймовірність ризиків за допомогою нечіткої логіки і Байєсової мережі (кроки 3–4); оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків (крок 5). Ця модель забезпечує комплексне управління вимогами кібербезпеки під час

впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків [13] – [15].

ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МОДЕЛІ НА ОСНОВІ ВИМОГ МІЖНАРОДНОГО СТАНДАРТУ NIST 800-53

Для детального прикладу візьмемо загальний бюджет у розмірі 1,000,000 грн і розподілимо його між вимогами кібербезпеки на основі стандартів NIST, використовуючи запропоновану модель управління вимогами. Припустимо, що мета — оптимально розподілити кошти між вимогами кібербезпеки, мінімізуючи ризики, і водночас забезпечити високий рівень виконання кожної вимоги.

Вихідні дані прикладу:

Вимоги:

1. **Контроль доступу (AC)** — обмеження доступу до даних.
2. **Захист цілісності даних (SI)** — забезпечення цілісності зберігання даних.
3. **Реагування на інциденти (IR)** — заходи для своєчасного реагування.
4. **Аудит і логування (AU)** — запис подій для моніторингу та контролю.

Бюджет і ресурсні обмеження:

- **Загальний бюджет**: 1,000,000 грн.
- **Вартість виконання вимог** (у разі повного фінансування):
  AC: 300,000 грн
  SI: 400,000 грн
  IR: 200,000 грн
  AU: 100,000 грн.

Таблиця 1

Пріоритети вимог за важливістю та ризиком (метод AHP)

Вимога	Важливість W_i	Ризик R_i
AC	0.3	0.2
SI	0.4	0.4
IR	0.2	0.3
AU	0.1	0.1

Критерії для нечіткої логіки:

- **Висока відповідність**: $m_{high} = [0.8, 1.0]$
- **Середня відповідність**: $m_{medium} = [0.5, 0.7]$
- **Низька відповідність**: $m_{low} = [0, 0.4]$

Ймовірність виникнення загроз за Байєсовою мережею:

- **Фішинг-атака: 0.3, що впливає на AC.**
- **Витік даних: 0.5, що впливає на SI.**
- **Зловмисне ПЗ: 0.2, що впливає на IR.**

Кроки реалізації розробленої моделі:

Крок 1: Створення графу залежностей вимог

Граф залежностей:

- **IR** залежить від **AU** — для оперативного реагування потрібні журнали подій.

ISSN 2663 - 4023

– **SI** має критичний вплив на **AC** та **IR**, оскільки цілісність даних важлива для обох процесів.

Крок 2: Пріоритезація вимог за допомогою AHP

Загальна оцінка пріоритету для кожної вимоги за (1):

$$P_i = aW_i + bR_i,$$

де $a = 0.6$ (вага важливості) та $b = 0.4$ (вага ризику).

Таблиця 2

Пріоритетизація вимог

Вимога	**Пріоритет** P_i
AC	$0.6 \times 0.3 + 0.4 \times 0.2 = 0.26$
SI	$0.6 \times 0.4 + 0.4 \times 0.4 = 0.40$
IR	$0.6 \times 0.2 + 0.4 \times 0.3 = 0.24$
AU	$0.6 \times 0.1 + 0.4 \times 0.1 = 0.10$

Крок 3: Застосування нечіткої логіки для оцінки відповідності

Припустимо, що поточний рівень виконання вимог оцінюється наступним чином (табл. 3):

Таблиця 3

Рівень виконання вимог

Вимога	**Відповідність** x_i
AC	0.7
SI	0.85
IR	0.6
AU	0.5

На основі цього відповідність оцінюється як:

– **AC: Середня відповідність**

– **SI: Висока відповідність**

– **IR: Середня відповідність**

– **AU: Середня відповідність**

Крок 4: Моделювання ризиків за допомогою Байєсової мережі

Обчислюємо ймовірність компрометації для кожної вимоги з урахуванням її відповідності:

– **AC**: $P(compromised) = 0.3 \cdot (1 - 0.7) = 0.09$

– **SI**: $P(compromised) = 0.5 \cdot (1 - 0.85) = 0.075$

– **IR**: $P(compromised) = 0.2 \cdot (1 - 0.6) = 0.08$

– **AU**: $P(compromised) = 0.5$ (при незначному ризику).

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Цільова функція:

$$min \sum_{i=1}^{n} (1 - x_i) \cdot P_i \cdot Risk(v_i),$$

Обмеження:

$$\sum_{i=1}^{n} x_i \cdot C_i \leq B,$$

де C_i — вартість виконання вимоги i, B =1 000 000 грн.

Розв'язуючи оптимізаційну задачу (за умови пропорційного розподілу ресурсів і врахування обмежень бюджету), отримуємо наступні значення оптимального виділення ресурсів (табл. 4).

Таблиця 4

Оптимальне виділення ресурсів

Вимога	Оптимальне виділення ресурсів (%)	Виділення коштів (грн)
AC	30%	300,000
SI	40%	400,000
IR	20%	200,000
AU	10%	100,000

Результати реалізації моделі на основі стандарту NIST 800-53

- **Вимоги AC та SI** отримали найбільше фінансування (30% і 40% бюджету відповідно), що відповідає їхнім високим пріоритетам за критеріями важливості та ризику.
- **IR** отримала 20% фінансування, що забезпечує достатній рівень виконання та знижує ризик від зловмисного ПЗ.
- **AU** отримала 10% фінансування, що дозволяє підтримувати базовий рівень аудиту та логування.

Таким чином, модель управління вимогами кібербезпеки при впровадженні ПЗ забезпечила мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно зі стандартами NIST.

ВИСНОВКИ

Отже, в роботі було проведено дослідження математичних методів для управління вимогами кібербезпеки при впровадженні ПЗ. Було розроблено модель, яка дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків за допомогою нечіткої логіки і Байєсової мережі, а також оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків. Запропонована авторами модель складається з наступних етапів: створення графу залежностей вимог, використання методу AHP для пріоритезації вимог, застосування нечіткої логіки для оцінки рівня відповідності вимогам, моделювання ризиків за допомогою Байєсової мережі, оптимізація ресурсів за допомогою математичного програмування. Розроблена модель забезпечує комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків.

Експериментальне дослідження розробленої моделі, було проведено на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно зі стандартами NIST. Зокрема, встановлено:

- Вимоги AC та SI отримали найбільше фінансування (30% і 40% бюджету відповідно), що відповідає їхнім високим пріоритетам за критеріями важливості та ризику.
- IR отримала 20% фінансування, що забезпечує достатній рівень виконання та знижує ризик від зловмисного ПЗ.
- AU отримала 10% фінансування, що дозволяє підтримувати базовий рівень аудиту та логування.

Подальші дослідження будуть спрямовані на оптимізацію моделі та її практичну реалізацію для інших сучасних міжнародних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Li, L., et al. (2024). LogicEdu: Enhancing computational logic understanding through web-based Boolean logic simplification tool. *2024 21st International SoC Design Conference (ISOCC)*, Sapporo, Japan, 390–391. https://doi.org/10.1109/ISOCC62682.2024.10762040
2. Deepak, S., Shah, J. A., Chetan, N., & Sharda, H. (2023). New decision-making process based on set theory: Towards application of set theory. *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, 1–6. https://doi.org/10.1109/ICTBIG59752.2023.10456045
3. Wang, H. (2022). Network graph theory and organization model analysis based on mathematical modeling with the dynamic systematic data perspective. *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 915–919. https://doi.org/10.1109/ICOEI53556.2022.9776767
4. Bhadra, S. (2022). A stochastic Petri net model of continuous integration and continuous delivery. *2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Charlotte, NC, USA, 114–117. https://doi.org/10.1109/ISSREW55968.2022.00050
5. Suresh Kumar, K., Sudha, R., Suguna, T., & Dharani, M. K. (n.d.). An intelligent heartbeat management system utilizing fuzzy logic. In *Advances in Fuzzy-Based Internet of Medical Things (IoMT)*, 211–223. Wiley. https://doi.org/10.1002/9781394242252.ch14
6. Yu, Q., & Li, Z. (2020). A Bayesian model averaging method for software reliability assessment. *2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM)*, Vancouver, BC, Canada, 1–5. https://doi.org/10.1109/APARM49247.2020.9209504
7. Yang, B., et al. (2024). A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges. *Protection and Control of Modern Power Systems.* https://doi.org/10.23919/PCMP.2024.000297
8. Shukla, P., Singh, S. K., Khamparia, A., & Goyal, A. (n.d.). Nature-inspired optimization techniques. In *Nature-Inspired Optimization Algorithms: Recent Advances in Natural Computing and Biomedical Applications*, 137–152. De Gruyter.
9. Beniwal, R., Kumar, V., & Sharma, V. (2024). Metaheuristics approaches towards secure and optimized routing in IoT: A systematic literature review. *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, Greater Noida, India, 1–6. https://doi.org/10.1109/ICEECT61758.2024.10739076
10. Zin, T. T., Moe, A. S. T., Phyo, C. N., & Tin, P. (2024). Fusion of strategic queueing theory and AI for smart city telecommunication system. *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*, Seoul, Republic of Korea, 653–657. https://doi.org/10.1109/MASS62177.2024.00104
11. Zhang, N., Chen, Y., Yang, W., Zhang, Z., Liu, Y., & Mao, W. (2021). Application of fault tree analysis for reliability evaluation and weak link identification of stadium power supply system using Monte Carlo simulation. *2021 IEEE Sustainable Power and Energy Conference (iSPEC)*, Nanjing, China, 4209–4214. https://doi.org/10.1109/iSPEC53008.2021.9735815
12. Kim, D., Jeon, B., & Koo, K. C. (2023). Addressing timely AI technology standardization challenges through a hierarchical analysis approach. *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Republic of Korea, 1431–1433. https://doi.org/10.1109/ICTC58733.2023.10393654

13. Sydorenko, V., Gnatyuk, S., Tolbatov, A., Fesenko, A., Yevchenko, Y., & Sotnichenko, Y. (2020). Experimental FMECA-based assessment of the critical information infrastructure importance in aviation. *CEUR Workshop Proceedings*, 2732, 136–156.
14. Hnatyuk, S. O., Berdybayev, R. Sh., Sydorenko, V. M., Zhigarevych, O. K., & Smirnova, T. V. (2023). Event correlation and cybersecurity incident management system at critical infrastructure facilities. *Cybersecurity: Education, Science, Technology*, 3(19), 176–196.
15. Polozhentsev, A. A., & Sydorenko, V. M. (2024). IT threat management method for critical information infrastructure facilities. *Science-Intensive Technologies*, 2(62), 143–153.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Sergiy Gnatyuk
Doctor of Technical Sciences, Professor, Vice-Rector for Research and Technology Transfer
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@kai.edu.ua

Viktoriia Sydorenko
PhD, Associate Professor, Associate Professor of the Department of Computer Information Technologies
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Anatolii Skurativskyi
Postgraduate Student
State University «Kyiv Aviation Institute», Kyiv, Ukraine
ORCID ID: 0009-0000-0566-2394
a.skurativskyi@gmail.com

CYBERSECURITY MANAGEMENT MODEL FOR SOFTWARE IMPLEMENTATION

Abstract. In today's digital world, cybersecurity has become a critical factor in software implementation across various domains. The increasing complexity of systems, the dynamic threat landscape, and limited resources require software developers and stakeholders to adopt effective mechanisms for managing cybersecurity requirements. This article presents an integrated mathematical model for managing cybersecurity requirements during software implementation. The relevance of this problem is driven by the growing complexity of modern information systems, the need for compliance with international security standards, and resource constraints during project execution. The proposed model combines several mathematical techniques, including the Analytic Hierarchy Process (AHP), fuzzy logic, Bayesian networks, and mathematical programming, ensuring a systematic decision-making approach. The model developed by the authors enables prioritization of requirements, evaluation of compliance under uncertainty, risk modeling, and optimal resource allocation while considering budget constraints and security objectives. An experimental study based on the NIST SP 800-53 standard confirmed the effectiveness of the proposed approach in reducing risks without exceeding available resources. The results are practically significant for organizations implementing software solutions in alignment with modern cybersecurity requirements. Future research will focus on optimizing the model and applying it to other international standards.

Keywords: cybersecurity, management model, management requirements, risk modeling, risk assessment, requirements prioritization, software, fuzzy logic, Bayesian network, mathematical programming, resource optimization, international standards, cybersecurity standards.

REFERENCES

1. Li, L., et al. (2024). LogicEdu: Enhancing computational logic understanding through web-based Boolean logic simplification tool. *2024 21st International SoC Design Conference (ISOCC)*, Sapporo, Japan, 390–391. https://doi.org/10.1109/ISOCC62682.2024.10762040
2. Deepak, S., Shah, J. A., Chetan, N., & Sharda, H. (2023). New decision-making process based on set theory: Towards application of set theory. *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, 1–6. https://doi.org/10.1109/ICTBIG59752.2023.10456045
3. Wang, H. (2022). Network graph theory and organization model analysis based on mathematical modeling with the dynamic systematic data perspective. *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 915–919. https://doi.org/10.1109/ICOEI53556.2022.9776767
4. Bhadra, S. (2022). A stochastic Petri net model of continuous integration and continuous delivery. *2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Charlotte, NC, USA, 114–117. https://doi.org/10.1109/ISSREW55968.2022.00050

5. Suresh Kumar, K., Sudha, R., Suguna, T., & Dharani, M. K. (n.d.). An intelligent heartbeat management system utilizing fuzzy logic. In *Advances in Fuzzy-Based Internet of Medical Things (IoMT)*, 211–223. Wiley. https://doi.org/10.1002/9781394242252.ch14
6. Yu, Q., & Li, Z. (2020). A Bayesian model averaging method for software reliability assessment. *2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM)*, Vancouver, BC, Canada, 1–5. https://doi.org/10.1109/APARM49247.2020.9209504
7. Yang, B., et al. (2024). A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges. *Protection and Control of Modern Power Systems.* https://doi.org/10.23919/PCMP.2024.000297
8. Shukla, P., Singh, S. K., Khamparia, A., & Goyal, A. (n.d.). Nature-inspired optimization techniques. In *Nature-Inspired Optimization Algorithms: Recent Advances in Natural Computing and Biomedical Applications*, 137–152. De Gruyter.
9. Beniwal, R., Kumar, V., & Sharma, V. (2024). Metaheuristics approaches towards secure and optimized routing in IoT: A systematic literature review. *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, Greater Noida, India, 1–6. https://doi.org/10.1109/ICEECT61758.2024.10739076
10. Zin, T. T., Moe, A. S. T., Phyo, C. N., & Tin, P. (2024). Fusion of strategic queueing theory and AI for smart city telecommunication system. *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*, Seoul, Republic of Korea, 653–657. https://doi.org/10.1109/MASS62177.2024.00104
11. Zhang, N., Chen, Y., Yang, W., Zhang, Z., Liu, Y., & Mao, W. (2021). Application of fault tree analysis for reliability evaluation and weak link identification of stadium power supply system using Monte Carlo simulation. *2021 IEEE Sustainable Power and Energy Conference (iSPEC)*, Nanjing, China, 4209–4214. https://doi.org/10.1109/iSPEC53008.2021.9735815
12. Kim, D., Jeon, B., & Koo, K. C. (2023). Addressing timely AI technology standardization challenges through a hierarchical analysis approach. *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Republic of Korea, 1431–1433. https://doi.org/10.1109/ICTC58733.2023.10393654
13. Sydorenko, V., Gnatyuk, S., Tolbatov, A., Fesenko, A., Yevchenko, Y., & Sotnichenko, Y. (2020). Experimental FMECA-based assessment of the critical information infrastructure importance in aviation. *CEUR Workshop Proceedings*, 2732, 136–156.
14. Hnatyuk, S. O., Berdybayev, R. Sh., Sydorenko, V. M., Zhigarevych, O. K., & Smirnova, T. V. (2023). Event correlation and cybersecurity incident management system at critical infrastructure facilities. *Cybersecurity: Education, Science, Technology*, 3(19), 176–196.
15. Polozhentsev, A. A., & Sydorenko, V. M. (2024). IT threat management method for critical information infrastructure facilities. *Science-Intensive Technologies*, 2(62), 143–153.