**DOI: 10.18372/2410-7840.21.13704**
**УДК 004.056.5**

# ОЦІНКА ПРІОРИТЕТІВ МЕХАНІЗМІВ КІБЕРЗАХИСТУ НАЦІОНАЛЬНОЇ СИСТЕМИ ОПЛАТИ КОМУНАЛЬНИХ ПОСЛУГ ЗА ДОПОМОГОЮ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

***Мирослава Стремецька***

*В умовах зростання попиту на розробку комунікаційних систем, спрямованих на задоволення суспільних потреб, реалізацію електронних державних послуг, електронної комерції та електронного документообігу, виникає гостра необхідність в побудові Мирослава Стремецька організаційно-технічних моделей кібербезпеки як комплексу заходів, сил і засобів для їх кіберзахисту. Важливо, щоб запропонований підхід до розробки таких моделей був не лише універсальним для всіх об'єктів кіберзахисту, а й враховував цілком конкретні особливості функціонування кожної окремої системи. Розроблено ієрархічну модель системи забезпечення безпеки (СЗБ) національної системи оплати комунальних послуг, що враховує як технологічні особливості окремих складових підсистем, так і принципи їх взаємодії з точки зору головної цілі – досягнення стану захищеності системи загалом. На основі побудованої моделі виконано оцінку пріоритетів механізмів кіберзахисту за допомогою методу аналізу ієрархій (МАІ). Методологія дозволяє реалізувати системний підхід до побудови організаційно-технічних моделей складних ієрархічних систем; дозволяє отримати кількісні оцінки пріоритетів рішень, спираючись на які можна формалізувати процедуру вибору тих чи інших сценаріїв роботи СЗБ; допомагає сформувати математичний апарат для дослідження низки інших складних об'єктів кіберзахисту в рамках національної системи кібербезпеки держави.*

***Ключові слова:*** *метод аналізу ієрархій (МАІ), матриця попарних порівнянь, вектор пріоритетів, відношення узгодженості, національна система оплати комунальних послуг, система забезпечення безпеки (СЗБ).*

**Вступ**

Визначальними передумовами для сталого розвитку України є поліпшення безпеки мереж та використання інформаційно-комунікаційних технологій (ІКТ) приватними особами, бізнесом та адміністративними органами шляхом впровадження онлайн-послуг, зокрема електронного бізнесу, електронного уряду, що закріплено Угодою про асоціацію між Україною та ЄС, ратифіковану 16.09.2014 р. [9]. В рамках реалізації даної стратегії сформувалась гостра потреба в розробці нових ефективних підходів до організації СЗБ в кіберпросторі, що в повній мірі враховуватимуть технологічну складність об'єктів кіберзахисту.

Попередні дослідження з даного напрямку [7, 8] показали, що в питаннях кіберзахисту складних багаторівневих розгалужених інформаційних систем важливо, по-перше, запропонувати релевантну організаційно-технічну модель СЗБ, а по-друге, забезпечити підтримку процесу прийняття рішень щодо вибору того чи іншого сценарію роботи СЗБ. В свою чергу, МАІ виступає математичною моделлю складних ієрархічних систем [6], що дає можливість отримати кількісні оцінки пріоритетів рішень, спираючись на які можна формалізувати процедуру вибору тих чи інших сценаріїв роботи СЗБ.

Таким чином, доцільно реалізувати системний підхід до побудови організаційно-технічних моделей СЗБ таких складних ієрархічних систем, як, наприклад, національна система оплати комунальних послуг, за допомогою МАІ. Важливо, щоб отримана модель враховувала як технологічні особливості окремих складових підсистем [4], так і принципи їх взаємодії з точки зору головної цілі – досягнення стану захищеності системи [2], формуючи при цьому чітке уявлення щодо ступеню впливу окремих механізмів кіберзахисту на досягнення загальної цілі.

**Мета роботи**

Розробити ієрархічну модель СЗБ національної системи оплати комунальних послуг, що враховує як технологічні особливості окремих складових підсистем, так і принципи їх взаємодії в цілому. На основі побудованої ієрархічної моделі виконати оцінку пріоритетів механізмів кіберзахисту за допомогою МАІ.

**Наукова новизна** визначається наступними результатами: побудовано ієрархічну модель СЗБ національної системи оплати комунальних послуг; отримано кількісні оцінки пріоритетів механізмів кіберзахисту для даної моделі, що дозволяє сформувати математичний апарат для дослідження низки інших об'єктів кіберзахисту в рамках національної системи кібербезпеки держави.

**1. Методика МАІ**

Концепція МАІ, запропонована відомим американським математиком Томасом Л. Сааті, спрямована на потреби формулювання низки простих та універсальних кроків, слідуючи яким особа, що

приймає рішення (ОПР), зможе провести глибокий аналіз проблем найрізноманітнішої складності, і як результат, - забезпечити безпосередню підтримку процесу прийняття рішень.

Метод сформувався в результаті комбінації двох підходів:

– побудови ієрархії цілей, а також заходів, сил і засобів для їх досягнення, з метою проведення експертом подальшої оцінки ефективності можливих сценаріїв дій для досягнення загальної цілі;

– ранжування експертних оцінок засобами матричного аналізу.

Таким чином, ідея такого методу полягає в «ієрархічній декомпозиції задачі прийняття рішення з досліджуваної проблеми з подальшим багатокритеріальним рейтингуванням альтернатив, із яких обирається одна як рішення» [6].

Ключовою структурою, у вигляді якої подається проблема прийняття рішення, є ієрархія, що будується у вигляді впорядкованих:

– загальної цілі, що виступає головним критерієм рейтингування можливих рішень;

– груп (або рівнів) однотипних та незалежних в рамках одного рівня чинників, що за класифікацією Т. Сааті називаються «Сили» (або «Технології»), «Актори» та «Цілі» (в свою чергу, кожен елемент таких рівнів також виступає критерієм для локального рейтингування пов'язаних з ним елементів попереднього рівня ієрархії);

– групи (або рівня) можливих «Глобальних проблем», рішення яких необхідне для досягнення загальної цілі (відповідає множині альтернативних варіантів рішень або альтернатив);

– системи однонаправлених зв'язків між сусідніми рівнями.

Структури такого типу мають ряд ключових переваг перед мережами, логічними ланцюгами чи іншими способами моделювання систем, зокрема, особливої уваги заслуговує їх стійкість (малі зміни викликають малий ефект) та гнучкість (внесення нових елементів у добре структуровану ієрархію не руйнує характеристик загальної системи), що дозволяє аналітикам експериментувати зі структурою окремих деталей, не завдаючи суттєвої шкоди архітектурі в цілому.

**2. Ієрархічна модель СЗБ національної системи оплати комунальних послуг**

Застосуємо метод аналізу ієрархій до задачі побудови організаційно-технічної моделі кібербезпеки національної системи оплати комунальних послуг. Слід звернути увагу, що наведена система включає досить велику кількість внутрішніх підсистем, пов'язаних між собою мережею як фізичних, так і логічних зв'язків. Це дозволяє провести ефективне випробування методу на системі реального рівня складності, а також може використовуватись як основа для побудови організаційно-технічних моделей кібербезпеки інших об'єктів кіберзахисту, що мають спільні структурні елементи.

Розглянемо архітектуру такої системи докладніше (Рис. 1). Для початку, слід виділити в системі 3 адміністративні рівні: національний, обласний та клієнтський. На національному рівні система складається з потужного центру обробки даних (ЦОДу) та локальної обчислювальної мережі (англ. Local Area Network, LAN), що його обслуговує. Доступ до внутрішніх сервісів локальної мережі ЦОД всіх зовнішніх сервісів системи відбувається через міжмережевий файєрвол Cisco ASA 5555-X, при цьому ресурси зовнішніх сервісів відділяються в окремі спеціалізовані сегменти мережі в рамках інформаційного периметру LAN– демілітаризовані зони (англ. Demilitarized Zone, DMZ). На обласному рівні запропоновано розмістити головні центри обслуговування (ЦО) клієнтів, що підтримуватимуть роботу системи на території окремої області чи багатомільйонного міста. Такі центри будуть представлені у всіх куточках підзвітної їм території регіональними представництвами, що матимуть достатньо обчислювальних потужностей для забезпечення обміну інформацією з національним ЦОДом по захищеному VPN-каналу (англ. Virtual Private Network) та проведення оплати комунальних послуг в режимі реального часу засобами системи електронних платежів (СЕП) на базі CP (англ. Card Present) транзакцій та готівкою [8]. В свою чергу, клієнтський рівень представляє собою встановлення спеціально розробленого мобільного додатка на смартфони чи інші персональні гаджети, або використання веб-додатку, за допомогою яких мешканці всієї України зможуть проводити оплату комунальних послуг в режимі реального часу засобами СЕП на базі CNP (англ. Card not Present) транзакцій. До цього ж рівня можна віднести впровадження датчиків (сенсорів) збору даних, інтегрованих з лічильниками комунальних послуг, що зможуть передавати дані показників лічильників до бази даних (БД) національного ЦОД в режимі онлайн за допомогою системи GSM-зв'язку (англ. Global System for Mobile Communications).

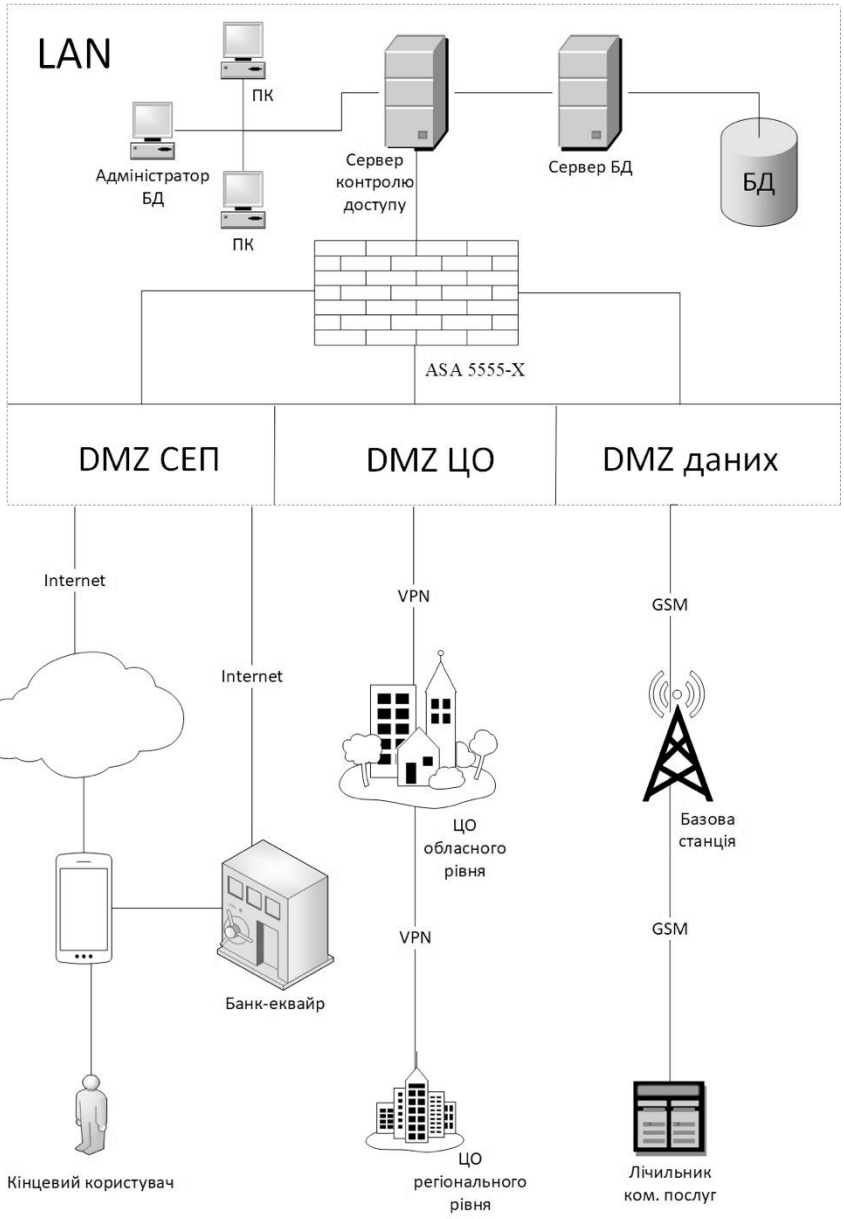


Рис. 1. Структура національної системи оплати комунальних послуг з підтримкою СЕП та підсистеми збору даних з лічильників комунальних послуг

Спираючись на зображену модель, здійснимо докладний аналіз комплексу заходів, сил і засобів, необхідних для досягнення стану захищеності розглянутої інформаційно-телекомунікаційної системи.

Для цього скористаємось методом аналізу ієрархій щодо задачі побудови СЗБ національної системи оплати комунальних послуг. Як і в класичній моделі МАІ, будуємо ієрархію, що складається з п'яти рівнів: «Загальна ціль», «Сили», «Актори», «Цілі» та «Глобальні проблеми». В рамках кожної групи виділяємо низку однотипних, але незалежних елементів, що пов'язані мережею зв'язків з елементами сусідніх рівнів (Рис. 2).

**Перший рівень ієрархії.** Складається з єдиного елемента, що представляє загальну ціль, яку необхідно досягнути в результаті прийняття рішення, а саме: досягнення стану захищеності (безпека) національної системи оплати комунальних послуг.

**Другий рівень ієрархії**. Відповідає набору технологій, використаних в процесі побудови національної системи оплати комунальних послуг, і захист яких відповідає досягненню загальної цілі рівня І. Зокрема, критично важливими для роботи системи є технології, пов'язані з системами електронних платежів на базі CP та CNP транзакцій [7, 8]; веб-додатків та мобільних додатків, необхідних для проведення оплати та перегляду стану рахунків комунальних послуг кінцевими користувачами в режимі онлайн; мережеві та хмарні технології, технології GSM-передачі даних.

**Третій рівень ієрархії.** Відображає конкретні елементи в архітектурі національної системи

оплати комунальних послуг, кожен із яких відповідає за низку життєво важливих для системи функцій: центри надання послуг обласного та регіонального рівня; платіжна система, що об'єднує всі можливі способи електронної оплати; мобільні та веб-додатки як портали для роботи з клієнтами; центр обробки даних як головна система обробки всіх інформаційних потоків; портали для обміну даними з компаніями-постачальниками комунальних послуг, а також сенсори даних, що передаватимуть показники лічильників до головного ЦОДу.

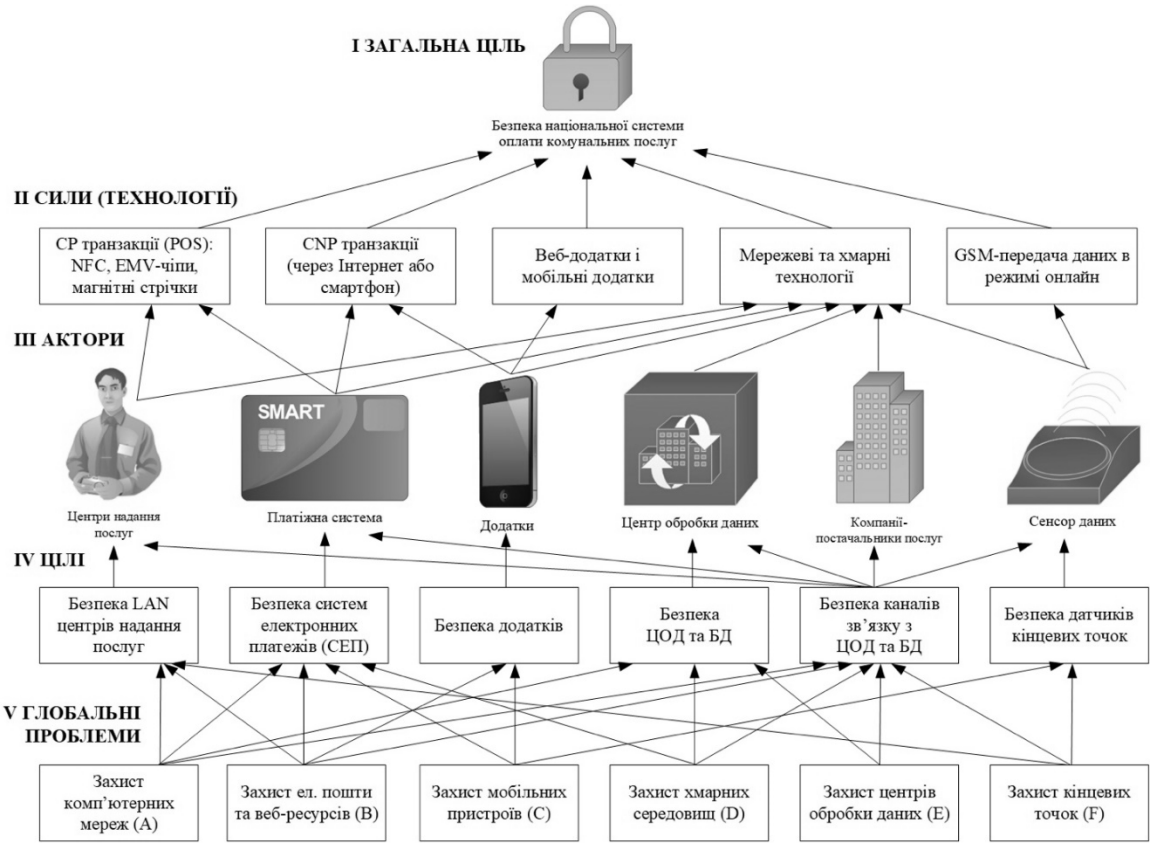


Рис. 2. Ієрархічна модель MAI

**Четвертий рівень ієрархії.** За аналогією до третього рівня, кожному актору відповідає конкретна ціль: забезпечити безпеку локальних мереж центрів надання послуг, СЕП, мобільних та веб-додатків, ЦОДу разом із власною БД, каналів зв'язку з ЦОДом та БД всіх акторів, а також датчиків кінцевих точок для обміну даними з лічильниками комунальних послуг відповідно.

**П'ятий рівень ієрархії.** Реалізує рішення ОПР щодо захисту тих чи інших сегментів системи, відкриваючи глобальну проблематику, описану в портфоліо провідних вендорів ринку кіберзахисту [10], зокрема:

1. Захист комп'ютерних мереж (A), що включає захист LAN та розподіленої комп'ютерної мережі центрів надання послуг, захист каналів зв'язку з ЦОД та БД, а також захист СЕП (зокрема від загроз зі сторони мережі Інтернет);

2. Захист електронної пошти та веб-ресурсів (B) передбачає захист корпоративної пошти, користувачами якої є, зокрема, співробітники центрів обслуговування, а також захист веб-додатку та пов'язаних з ним СЕП на базі CNP транзакцій;

3. Захист мобільних пристроїв (C) визначає в т. ч. механізми захисту мобільних додатків та пов'язаних з ним СЕП на базі CNP транзакцій, а також захист датчиків кінцевих точок (що з огляду на свої технічні особливості та спосіб обміну даними демонструє, окрім іншого, ознаки мобільного пристрою);

4. Захист хмарних середовищ (D) дозволяє безпечно використовувати обчислювальні ресурси та пам'ять віддалених хмарних середовищ для потреб ЦОД та БД, і за потреби, для обслуговування СЕП на базі CNP транзакцій;

5. Захист центрів обробки даних (E) передбачає застосування механізмів захисту як безпосередньо самого ЦОДу, так і для захисту з'єднань з ЦОД всіх акторів з використанням механізмів контролю доступу до БД;

6. Захист кінцевих точок (F) визначає механізми захисту сенсорів та їх систем передачі даних, а також, робочих станцій кінцевих користувачів у розподіленій корпоративній мережі.

Очевидно, що не існує єдиного вірного сценарію щодо захисту тих чи інших елементів системи, проте дана ієрархія за рахунок вертикальних зв'язків наочно демонструє, як ті чи інші механізми кіберзахисту впливають на реалізацію загальної цілі - досягнення стану захищеності (безпеку) національної системи оплати комунальних послуг.

**3. Формування експертних оцінок та ієрархічний синтез МАІ**

На наступному етапі застосування МАІ експерт (експерти), спираючись на побудовану ієрархічну модель (Рис. 2), зможуть отримати кількісні оцінки розглянутих сценаріїв за рівнем впливу на сформульовану загальну ціль [3, 5]. Згідно з методом МАІ, експерт проводить парні порівняння елементів, що знаходяться на одному рівні ієрархії відносно спільного елемента вищого рівня. Парні порівняння проводяться у фундаментальній шкалі відносної важливості Т. Сааті, побудованого на основі психофізичного закону Вебера-Фехнера [6, ст.19]. Для цього, починаючи з рівня Сил (Технологій), експерти відповідають на наступні запитання:

– **Другий рівень ієрархії.** «Яка з використаних технологій найбільш суттєво впливає на ризики безпеки національної системи оплати комунальних послуг?».

– **Третій рівень ієрархії.** «Інтереси кого з акторів найбільш тісно пов'язані з застосуванням відповідних технологій?».

– **Четвертий рівень ієрархії.** «Які цілі найбільш суттєві з точки зору діючих сторін (акторів)?».

– **П'ятий рівень ієрархії.** «Які проблеми необхідно розв'язати в першу чергу для досягнення конкретних цілей?».

За результатами проведених експертом парних порівнянь формуються матриці парних порівнянь (МПП) виду: $A = \|\alpha_{ij}\|, (i = \overline{1,n}; j = \overline{1,n})$. Наприклад, $A_2$ визначено як МПП елементів рівня II відносно єдиного елементу рівня I - Таблиця 1. Далі для кожної МПП за методом головного власного вектору [1, ст. 201] визначається вектор локальних пріоритетів $w = (w_1, w_2, \dots, w_n)^T$:

$$w_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}} \Big/ \sum_{i=1}^{n} \left( \sqrt[n]{\prod_{j=1}^{n} a_{ij}} \right), \quad i = \overline{1,n}.$$

Вектори локальних пріоритетів елементів одного рівня зводяться у матриці локальних пріоритетів критеріїв (для рівнів II, III, IV) або альтернатив (для рівня V) - Таблиця 1. Якщо $w^{(j)} = (w_1{}^{(j)}, w_2{}^{(j)}, \dots, w_n{}^{(j)})^T$ – вектор локальних пріоритетів елементів рівня k відносно j-го критерія рівня k-1, то матриця локальних пріоритетів елементів рівня k визначається за формулою: $LP_k = \|p_{ij} = w_i{}^{(j)}\|, i = \overline{1,n};\ j = \overline{1,m}$, де n - кількість елементів рівня k; m - кількість елементів рівня k-1.

Головним завданням МАІ є визначення глобальних пріоритетів альтернатив, тобто їх пріоритетів відносно кореня ієрархії. Для цього на останньому етапі за процедурою ієрархічного синтезу [1, ст. 210] обчислено вектор глобальних пріоритетів альтернатив $W = W_5$ (Таблиця 1) відносно загальної цілі (кореня ієрархії) за формулою: $W_k = LP_k \times W_{k-1}$, де $k = 3{,}4{,}5; W_2 = LP_2$.

Здійснена оцінка послідовності тверджень експерта, в ході якої було обчислено відношення узгодженості $\mathrm{I_{u_0}}$ для усіх МПП [1, ст. 202] за формулою:

$$\mathrm{I_{u_0}} = \frac{\sum_{j=1}^{n}(w_j \times \sum_{i=1}^{n} a_{ij}) - n}{n-1} \cdot \frac{1}{M(\mathrm{I_u})} = \frac{\mathrm{I_u}}{M(\mathrm{I_u})},$$

де $M(\mathrm{I_u}) = \mathrm{const}$ - значення випадкової узгодженості, $\mathrm{I_u} = \sum_{j=1}^{n}(w_j \times \sum_{i=1}^{n} a_{ij}) - n \Big/ n - 1$ – індекс узгодженості матриці виду $A = \|\alpha_{ij}\|, (i = \overline{1,n}; j = \overline{1,n})$, Результати показали, що жоден з показників відношень узгодженості МПП не перевищив 10%.

Також обраховано узагальнене відношення узгодженості $\mathrm{I_{H_0}}$ на всю ієрархію. Якщо $\left(\mathrm{I_{u_k}^{(1)} I_{u_k}^{(2)} \dots I_{u_k}^{(n_{k-1})}}\right)^T$ – вектор-стовпчик індексів узгодженості МПП елементів рівня k, де $k = \overline{2,5}$ - номер рівня ієрархії, $n_{k-1}$ - кількість елементів рівня k-1. Тоді узагальнене відношення узгодженості $\mathrm{I_{H_0}}$ на всю ієрархію обчислюється за формулою:

$$\mathrm{I_{H_0}} = \left( \mathrm{I_{u_2}^{(1)}} + W_2{}^T \cdot \begin{pmatrix} \mathrm{I_{u_3}^{(1)}} \\ \mathrm{I_{u_3}^{(2)}} \\ \dots \\ \mathrm{I_{u_3}^{(5)}} \end{pmatrix} + W_3{}^T \cdot \begin{pmatrix} \mathrm{I_{u_4}^{(1)}} \\ \mathrm{I_{u_4}^{(2)}} \\ \dots \\ \mathrm{I_{u_4}^{(6)}} \end{pmatrix} + W_4{}^T \cdot \begin{pmatrix} \mathrm{I_{u_5}^{(1)}} \\ \mathrm{I_{u_5}^{(2)}} \\ \dots \\ \mathrm{I_{u_5}^{(6)}} \end{pmatrix} \right) \cdot \frac{1}{M(\mathrm{I_H})} = \frac{\mathrm{I_H}}{M(\mathrm{I_H})},$$

$$\text{де } M(I_H) = M(I_{u_2}^{(1)}) + W_2{}^T \cdot \begin{pmatrix} M(I_{u_3}^{(1)}) \\ M(I_{u_3}^{(2)}) \\ \dots \\ M(I_{u_3}^{(5)}) \end{pmatrix} + W_3{}^T \cdot \begin{pmatrix} M(I_{u_4}^{(1)}) \\ M(I_{u_4}^{(2)}) \\ \dots \\ M(I_{u_4}^{(6)}) \end{pmatrix} + W_4{}^T \cdot \begin{pmatrix} M(I_{u_5}^{(1)}) \\ M(I_{u_5}^{(2)}) \\ \dots \\ M(I_5^{(6)}) \end{pmatrix}.$$

Значення показника $I_{H_0}$ склало 3,47%, що вважається цілком задовільним. Тобто твердження експерта можна вважати послідовними і такими, яким можна довіряти.

Результати здійсненого аналізу демонструють, що найбільшу увагу ОПР слід приділяти захисту електронної пошти та веб-ресурсів (29,9%), що є досить раціональним, оскільки з цими сегментами системи пов'язані потенційні ризики щодо впливу на безпеку СЕП, а також розподіленої корпоративної мережі, користувачі якої є клієнтами корпоративної електронної пошти зокрема. На другому місці знаходиться захист комп'ютерних мереж (25,6%), третє місце посів захист мобільних пристроїв (19,53%), на четвертому місці – захист кінцевих точок (12,25%), і п'яте та шосте місце займають захист центрів обробки даних (7,99%) та захист хмарних середовищ (4,73%) відповідно (Рис. 3).

Таблиця 1

Ієрархічний синтез МАІ

| I-II рівні ієрархії МАІ | | | | | | | |
|---|---|---|---|---|---|---|---|
| Матриця попарних порівнянь критеріїв, $A_2$ | | | | | | | Вектор пріоритетів |
| | 1 | 2 | 3 | 4 | 5 | | $W_2 = LP_2$ |
| 1 | 1,00 | 0,50 | 2,00 | 0,33 | 0,50 | | 0,1249 |
| 2 | 2,00 | 1,00 | 2,00 | 0,50 | 2,00 | | 0,2358 |
| 3 | 0,50 | 0,50 | 1,00 | 0,33 | 0,50 | | 0,0946 |
| 4 | 3,00 | 2,00 | 3,00 | 1,00 | 2,00 | | 0,3660 |
| 5 | 2,00 | 0,50 | 2,00 | 0,50 | 1,00 | | 0,1787 |

| II-III рівні ієрархії МАІ | | | | | | | |
|---|---|---|---|---|---|---|---|
| Матриця локальних пріоритетів критеріїв (збірна), $LP_3$ | | | | | | | Вектор пріоритетів |
| | 1 | 2 | 3 | 4 | 5 | | $W_3$ |
| 1 | 0,87500 | 0,00000 | 0,00000 | 0,19379 | 0,00000 | | 0,1802 |
| 2 | 0,12500 | 0,25000 | 0,00000 | 0,12808 | 0,00000 | | 0,1214 |
| 3 | 0,00000 | 0,75000 | 1,00000 | 0,13703 | 0,00000 | | 0,3216 |
| 4 | 0,00000 | 0,00000 | 0,00000 | 0,29904 | 0,00000 | | 0,1095 |
| 5 | 0,00000 | 0,00000 | 0,00000 | 0,08068 | 0,00000 | | 0,0295 |
| 6 | 0,00000 | 0,00000 | 0,00000 | 0,16137 | 1,00000 | | 0,2378 |

| III-IV рівні ієрархії МАІ | | | | | | | |
|---|---|---|---|---|---|---|---|
| Матриця локальних пріоритетів критеріїв (збірна) ), $LP_4$ | | | | | | | Вектор пріоритетів |
| | 1 | 2 | 3 | 4 | 5 | 6 | $W_4$ |
| 1 | 0,8333 | 0,0000 | 0,0000 | 0,0000 | 0,0000 | 0,0000 | 0,1501 |
| 2 | 0,0000 | 0,8571 | 0,0000 | 0,0000 | 0,0000 | 0,0000 | 0,1041 |
| 3 | 0,0000 | 0,0000 | 1,0000 | 0,0000 | 0,0000 | 0,0000 | 0,3216 |
| 4 | 0,0000 | 0,0000 | 0,0000 | 0,2500 | 0,0000 | 0,0000 | 0,0274 |
| 5 | 0,1667 | 0,1429 | 0,0000 | 0,7500 | 1,0000 | 0,3333 | 0,2383 |
| 6 | 0,0000 | 0,0000 | 0,0000 | 0,0000 | 0,0000 | 0,6667 | 0,1585 |

| IV-V рівні ієрархії МАІ | | | | | | | |
|---|---|---|---|---|---|---|---|
| Матриця локальних пріоритетів альтернатив за критеріями (збірна), $LP_5$ | | | | | | | Вектор глобальних пріоритетів |
| | 1 | 2 | 3 | 4 | 5 | 6 | $W = W_5$ |
| 1 | 0,6483 | 0,4832 | 0,0000 | 0,3325 | 0,4167 | 0,0000 | 0,2560 |
| 2 | 0,1220 | 0,1569 | 0,7500 | 0,0000 | 0,0973 | 0,0000 | 0,2990 |
| 3 | 0,0000 | 0,0882 | 0,2500 | 0,0000 | 0,0000 | 0,6667 | 0,1953 |
| 4 | 0,0000 | 0,2717 | 0,0000 | 0,1396 | 0,0637 | 0,0000 | 0,0473 |
| 5 | 0,0000 | 0,0000 | 0,0000 | 0,5278 | 0,2749 | 0,0000 | 0,0799 |
| 6 | 0,2297 | 0,0000 | 0,0000 | 0,0000 | 0,1475 | 0,3333 | 0,1225 |

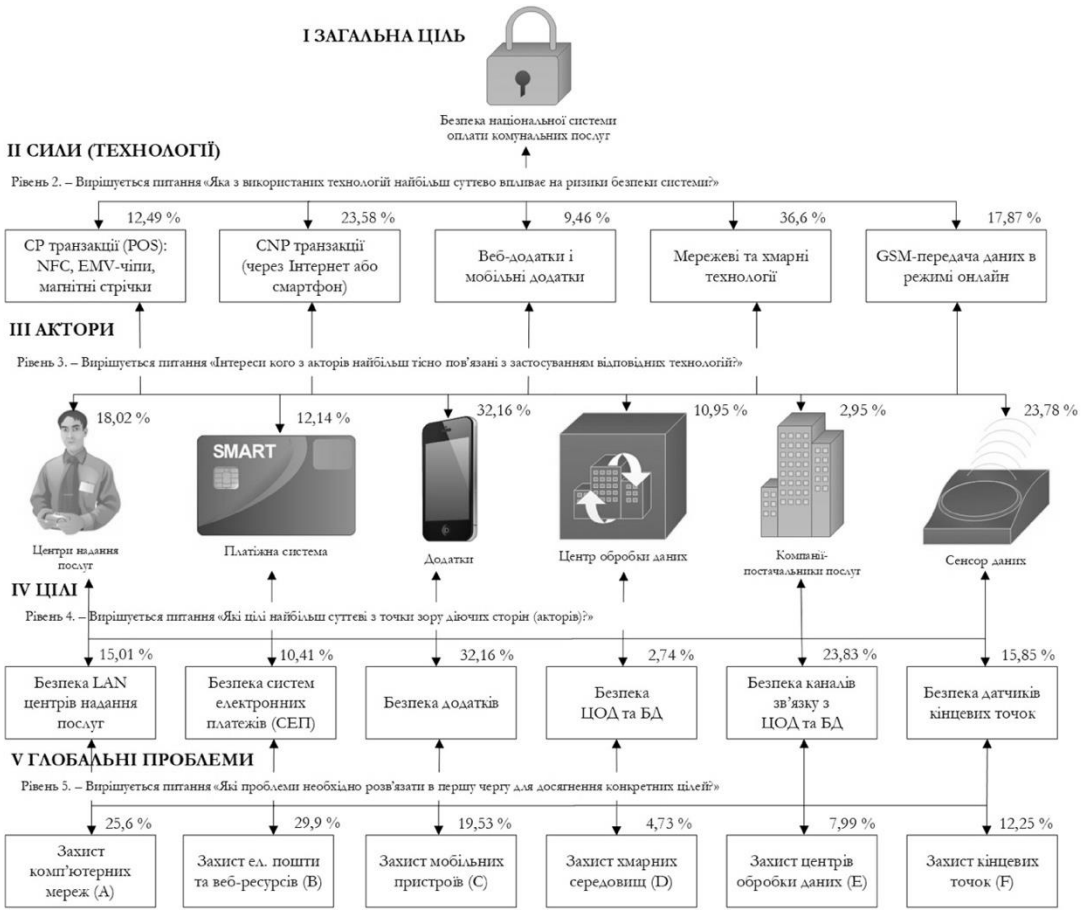


Рис. 3. Схема розподілу пріоритетів

Передбачається, що кожну проблему безпеки в подальшому можна розглядати з погляду сукупності альтернатив як комплексу заходів, сил і засобів для її рішення. Наприклад, що стосується захисту електронної пошти, традиційно виділяють: захист від спаму ($A_1$), антивірусне забезпечення ($A_2$), запобігання витоку даних (англ. Data Loss Prevention, DLP; $A_3$), шифрування ($A_4$) і т.д. відповідно до потенційного спектру кіберзагроз для даної системи.

Також, з метою підвищення об'єктивності та якості процедури прийняття рішень, рекомендують брати до уваги думку не одного, а декількох експертів. Для цього здійснюється групова експертиза з залученням додаткових фахівців у відповідній галузі знань. Підготовку такої процедури слід розпочати з розробки відповідних вимог до експертів та обрання механізму узгодження результатів опитувань. Ці та інші процедури заплановані в рамках подальшого аналітичного дослідження для побудови СЗБ національної системи оплати комунальних послуг.

**Висновки**

Реалізовано системний підхід до побудови організаційно-технічної моделі СЗБ національної системи оплати комунальних послуг за допомогою МАІ, в рамках якого:

1. Побудовано ієрархічну модель СЗБ національної системи оплати комунальних послуг, що враховує як технологічні особливості окремих складових підсистем, так принципи їх взаємодії в цілому;

2. На основі побудованої ієрархічної моделі засобами матричного аналізу проведено ієрархічний синтез МАІ, в результаті якого отримано оцінку пріоритетів механізмів кіберзахисту СЗБ національної системи оплати комунальних послуг.

Результати оцінювання демонструють, що з урахування локальних цілей найбільшу увагу ОПР слід приділяти захисту електронної пошти та веб-ресурсів (29,9%), на другому місці знаходиться захист комп'ютерних мереж (25,6%), третє місце посів захист мобільних пристроїв (19,53%), на четвертому місці – захист кінцевих точок (12,25%), і п'яте та шосте місце займають захист центрів обробки даних (7,99%) та захист хмарних середовищ (4,73%) відповідно.

З точки зору діючих сторін (акторів) найбільш суттєвими є наступні цілі: безпека додатків (32,16%), безпека каналів зв'язку з ЦОД та БД (23,83%), безпека датчиків кінцевих точок (15,85%), безпека LAN центрів надання послуг (15,01%), безпека СЕП (10,41%) і безпека ЦОД та БД (2,74%).

Що стосується технологічних інтересів системи, то ролі акторів відносно них розподілились наступним чином: додатки (32, 16%), сенсори даних (23,78%), центри надання послуг (18,02%), платіжна система (12,14%), ЦОД (10,95%), компанії-постачальники послуг (2,95%).

Стосовно важливості впливу на безпеку національної системи оплати комунальних послуг технології мають наступні пріоритети: мережеві та хмарні технології (36,6%), СЕП на базі CNP транзакцій (23,58%), GSM-передача даних в режимі онлайн (17,87%), СЕП на базі CP транзакцій (12,49%) та веб-додатки і мобільні додатки (9,46%).

Таким чином, МАІ дає чітке уявлення щодо інтересів СЗБ національної системи оплати комунальних послуг для забезпечення умов стабільного та всестороннього розвитку системи, забезпечує підтримку процесу прийняття рішень щодо вибору тих чи інших механізмів кіберзахисту для поетапного втілення сценарію роботи СЗБ.

Реалізація такої системної закономірності за рахунок ієрархічної будови системи дозволяє розв'язати проблему побудови СЗБ національної системи оплати комунальних послуг та допомагає сформувати математичний апарат для дослідження низки інших об'єктів кіберзахисту в рамках національної системи кібербезпеки держави.

## ЛІТЕРАТУРА


[1]. А. Катренко, В. Пасічник, В. Пасько, *Теорія прийняття рішень*, К.: ВНV, 2009, 448 с.

[2]. А. Качинський, *Безпека складних систем*, К.: ТОВ «Видавництво «Юстон», 2017, 498 с.

[3]. В. Матвиенко, *Прогностика: прогнозирование социальных и экономических процессов: теория, методика, практика*, К.: Українські пропілеї, 2000, 520 с.

[4]. Д. О'Конор, І. Макдермотт, *Системне мислення. Пошук неординарних творчих рішень*, К.: Наш формат, 2018, 240 с.

[5]. Н. Панкратова, Н. Недашківська, *Моделі і методи аналізу ієрархій. Теорія. Застосування*, К.: НТУУ «КПІ», 2010, 372 с.

[6]. А. Серіков, О. Білоцерківський, *Метод аналізу ієрархій у прийнятті рішень*: навч. посіб. для студ. вищ. навч. закл., Х.: Бурун книга, 2006, 144 с.

[7]. М. Стремецька, "Моделювання системи обробки інтенсивних розгалужених інформаційних потоків", *Матеріали XV Всеукраїнської науково-практичної конференції «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, 25-27 травня 2017 р., Київ: ПОЛІТЕХНІКА, С. 71-74, 2017.

[8]. М. Стремецька, А. Качинський, "Сучасні засоби захисту платіжних систем щодо обслуговування критичних сервісів держави", *Проблеми кібербезпеки інформаційно-комунікаційних систем: Збірник матеріалів доповідей та тез*, 05-06 квітня 2018 р., К.: ВПЦ «Київський університет», 2018, С. 174-177.

[9]. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]: [Угоду ратифіковано із заявою Законом № 1678-VII від 16.09.2014]. Режим доступу: https://zakon.rada.gov.ua/laws/show/984_011.

[10]. S. Hare, "Cisco's Attack Continuum", Ironshare, 22 April. [Electronic resource]. Online: https://www.ironshare.co.uk/technical/ciscos-attack-continuum/ (accessed 9 June2019).


## ОЦЕНКА ПРИОРИТЕТОВ МЕХАНИЗМОВ КИБЕРЗАЩИТЫ НАЦИОНАЛЬНОЙ СИСТЕМЫ ОПЛАТЫ КОМУНАЛЬНЫХ УСЛУГ С ПОМОЩЬЮ МЕТОДА АНАЛИЗА ИЕРАРХИЙ


В условиях повышения спроса на разработку коммуникационных систем, направленных на удовлетворение общественных потребностей, реализацию электронных государственных услуг, электронной коммерции и электронного документооборота, возникает острая необходимость в построении организационно-технических моделей кибербезопасности как комплекса мер, сил и средств для их киберзащиты. Важно, чтоб предложенный подход к разработке таких моделей был не только универсальным для всех объектов киберзащиты, но и учитывал вполне конкретные особенности функционирования каждой отдельной системы. Разработано иерархическую модель системы обеспечения безопасности (СОБ) национальной системы оплаты коммунальных услуг, которая учитывает, как технологические особенности отдельных составных подсистем, так и принципы их взаимодействия с точки зрения главной цели – достижения состояния защищенности системы в общем. На основе построенной модели выполнено оценку приоритетов механизмов киберзащиты с помощью метода анализа иерархий (МАИ). Методология позволяет реализовать системный подход к построению организационно-технических моделей сложных иерархических систем; позволяет получить количественные оценки приоритетов решений, опираясь на которые можно формализовать процедуру выбора тех или иных сценариев роботы СОБ; помогает сформировать математический аппарат для исследования ряда других сложных объектов киберзащиты в пределах национальной системы киберзащиты государства.



**Ключевые слова:** метод анализа иерархий (МАИ), матрица попарных сравнений, вектор приоритетов, отношение согласованности, национальная система оплаты коммунальных услуг, система обеспечения безопасности (СОБ).

**PRIORITIES EVALUATION OF CYBER DEFENSE MECHANISMS OF NATIONAL UTILITIES PAYMENT SYSTEM THROUGH THE USE OF THE ANALYTIC HIERARCHY PROCESS**

The article is devoted to the problem of evaluation of the influence of cyber defense mechanisms on the reaching security of national utilities payment system. With growing demand for the development of communication systems aimed at satisfying public needs, implementing e-government services, e-commerce and electronic document management there is an urgent need to construct organizational and technical cybersecurity models as a complex of measures, forces and means for their cyber defense. It was important that the proposed approach to the development of such models was not only one-size-fits-all to all objects of cyber defense and, most crucially, took into account very specific features of each individual system functioning. The Security Management System (SeMS) hierarchical model of national utilities payment system that included both the technological features of the individual subsystems and the guidelines for interaction between them in terms of the main objective - to achieve a safety state of the system, in general, was designed. The priorities evaluation of cyber defense mechanisms through the use of The Analytic Hierarchy Process (AHP) was performed based on the designed model. The results of evaluation showed that the first and foremost attention should be focused on e-mail and web security (29,9%), while computer network security (25,6%) got the second place, mobile security (19,53%) the third place, cyber defense mechanisms for endpoint protection (12,25%) the fourth place, data centers security (7,99%) the fifth place and cloud security (4,73%) the last place respectively. The methodology allows to implement a system approach to the construction of organizational and technical models of complex hierarchical systems; makes it possible to obtain quantitative scores of the decisions priorities, based on which it is possible to formalize the procedure of choosing the various scenarios for the work of the SeMS; helps to develop the appropriate mathematical apparatus for the study on number of other complex objects of cyber defense within the national cyber security system of Ukraine.

**Keywords:** Analytic Hierarchy Process (AHP), pairwise comparison matrix, score vector, Coherence Ratio (CR), National Utilities Payment System, Security Management System (SeMS).

**Стремецька Мирослава Станіславівна**, аспірант кафедри інформаційної безпеки Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: mira.stremetska@gmail.com.
Orcid ID: 0000-0003-0021-4300
**Стремецкая Мирослава Станиславовна**, аспирант кафедры информационной безопасности Физико-технического института Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
**Stremetska Myroslava**, PhD Student, Department of Information Security, Institute of Physics and Technology, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».