УДК 004.8:34 DOI 10.33111/mise.105.1

Бєгун А.В.,
к.е.н., професор кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана

Плахтій М. О.,
к.е.н., професор кафедри комп'ютерних наук,
Університет сучасних технологій

Biehun A.V.,
PhD in Economics, Professor, professor of the department
of system analysis and cyber security, KNEU named after Vadym Hetman
Plahtiy M. O.,
PhD, Professor of Department of Computer Science, University
of Modern Technologies

СПЕКТРАЛЬНА Р-МОДЕЛЬ ЗАХИСТУ ЕЛЕКТРОННИХ КВИТКІВ У ЦИФРОВИХ СЕРВІСНИХ СИСТЕМАХ

SPECTRAL P-MODEL OF PROTECTION OF ELECTRONIC TICKETS IN DIGITAL SERVICE SYSTEMS

Анотація*. З підвищенням популярності онлайн-сервісів спостерігається значне збільшення кількості інцидентів пов'язаних з атаками на системи електронних квитків. Тому зростає актуальність розробки ефективних моделей захисту в залежності від масштабованості та відкритості таких систем. Традиційні методи кібербезпеки не завжди спроможні забезпечити необхідний рівень захисту в умовах, коли постійно змінюються структури загроз. Цей факт вимагає нових підходів до аналізу і запобігання атак. Для виявлення закономірностей в атаках і формування ефективної стратегії захисту пропонується спектральна Р-модель, яка заснована на використанні спектральних методів аналізу, наприклад, перетворення Фур'є. В такому контексті Р- модель представляє собою математичний опис поведінки захисного процесу в частотній і часовій множинах; існує можливість прогнозувати загрози та адаптувати заходи протидії. Тобто, спектральна Р-модель спроможна : виявляти закономірності в поведінці зловмисників, аналізувати періодичність та інтенсивність атак, формувати адаптивні стратегії захисту в режимі реального часу. А це підвищить стійкість систем електронних квитків до зовнішніх впливів, забезпечить високий рівень надійності й безпеки в цифровому середовищі.*
Ключові слова*: система електронних квитків; спектральна Р-модель; інтерпретація спектру; кіберзагрози; предиктори атак; спектральні ознаки; точність виявлення.*

Abstract*. With the increasing popularity of online services, there is a significant increase in the number of incidents related to attacks on electronic ticket systems. Therefore, the relevance of developing effective protection models is increasing, depending on the scalability and openness of such systems. Traditional cybersecurity methods are not always able to*

provide the necessary level of protection in conditions where threat structures are constantly changing. This fact requires new approaches to analyzing and preventing attacks. To identify patterns in attacks and form an effective protection strategy, a spectral P-model is proposed, which is based on the use of spectral analysis methods, for example, the Fourier transform. In this context, the P-model is a mathematical description of the behavior of the protective process in frequency and time sets; it is possible to predict threats and adapt countermeasures. That is, the spectral P-model is able to: identify patterns in the behavior of attackers, analyze the frequency and intensity of attacks, and form adaptive protection strategies in real time. And this will increase the resistance of electronic ticket systems to external influences, ensure a high level of reliability and security in the digital environment.
***Keywords**: electronic ticket system; spectral P-model; spectrum interpretation; cyber threats; attack predictors; spectral features; detection accuracy.*

Вступ. Останнім часом електронні квитки стали невід'ємною частиною цифрової інфраструктури для організації та відвідування публічних заходів, конференцій, форумів, спортивних подій. Їх використання забезпечує зручність, автоматизацію процесів та зниження витрат. Однак, одночасно з цим зростає ризик кібератак, які направлені на підробку квитків, несанкціонований доступ та порушення функціонування систем обліку і розповсюдження квитків. Із зростанням популярності онлайн-сервісів відбувається значне збільшення кількості інцидентів, пов'язаних з атаками на системи електронних квитків. Тому актуальність розробки ефективних моделей захисту зростає пропорційно масштабованості та відкритості цих систем. Традиційні методи кібербезпеки не завжди спроможні забезпечити необхідний рівень захисту в умовах формування загроз, структури яких постійно змінюються та вимагають нових підходів до аналізу і запобігання атак.

Визначення цілей статті. В статті розглядається спектральна Р-модель нападу і захисту – математична модель, яка базується на використанні спектральних методів аналізу (наприклад, перетворення Фур'є) для виявлення закономірностей в атаках та проектування ефективної стратегії захисту. Р-модель в даному контексті представляє собою формалізований математичний опис поведінки атакуючого і захисного процесу у часовій та частотній сфері, що дозволяє прогнозувати загрози та адаптовано будувати заходи протидії.

Метою дослідження є розробка і теоретичне обгрунтування спектральної Р-моделі, яка спроможна:

- виявляти закономірності в поведінці зловмисників;
- аналізувати періодичність та інтенсивність атак;

- формувати адаптивні стратегії захисту в режимі реального часу.

Такий підхід дозволить підвищити сталість системи електронних квитків в умовах зовнішніх впливів, забезпечити високий рівень надійності безпеки у цифровому середовищі.

Викладення основного матеріалу. Відомо, що електронний квиток (e-ticket) представляє собою цифровий запис [1], який ідентифікує право користувача на участь в публічному заході. Сучасний електронний квиток зберігається у вигляді QR-кодів, штрих-кодів або токенів, які зчитуються на вході та порівнюються з базою даних організатора. Такі квитки можуть бути інтегровані в мобільні додатки, електронні гаманці або надсилаються електронною поштою. Такий стан електронного квитка зручний і корисний, але він має узагальнену множину можливостей для кіберзагроз:

- клонування квитків – копіювання унікального коду та його повторне використання;
- фішинг – отримання квитка обманним шляхом через підроблені сайти;
- несанкціонований доступ до бази даних квитків – підробка або спотворення квитків;
- DDoS-атаки на платформи продажу – тимчасове виведення системи з ладу, що ускладнює придбання і перевірку квитків.

В межах даної статі Р-модель представляє собою формальний математичний опис поведінки системи та взаємодіючих процесів: атакуючого (шкідливого) і захисного (реагуючого). Така модель описує наступне:

- вхідні параметри (інтенсивність атак, часові інтервали, типи атак);
- вихідні реакції системи захисту (детектування, ізоляція, поновлення);
- функції переходу між станами системи (наприклад, від «нормальної роботи» до «режиму загрози»).

Математично Р-модель може бути описана як система диференційних або різницевих рівнянь, де стани системи змінюються в часі під впливом зовнішніх збурень (атаки внутрішніх адаптивних механізмів захисту). Це дозволяє аналізувати стабільність і сталість системи при виникненні різноманітних сценаріїв.

Доведено [2], що спектральний аналіз – це метод дослідження сигналів або процесів у часовій та частотних сферах. Він дозволяє виявити:

- патерни, що повторюються (наприклад, атаки які відбуваються кожної хвилини);
- приховані закономірності (раптові сполохи, циклічні навантаження);
- предиктори атак (зростання активності в частотному діапазоні).

Застосування спектрального аналізу до кіберзагроз в системах електронних квитків надає можливість переходити від звичайного логування інцидентів до виявлення сталих ознак атакуючих стратегій, що критично важливо для їхнього раннього знаходження. В таких випадках доцільно використовувати швидке перетворення Фур'є (ШПФ) – алгоритм, який дозволяє ефективно обчислювати частотний спектр часових даних. Отримані частоти та амплітуди сигналів (наприклад, звернень до серверу, спроб автентифікації, транзакцій) можна використовувати для побудови поведінкової моделі атакуючого.

Спектральний аналіз загроз. Кібератаки на електронні квитки – це не хаотичні події, а процеси, які мають визначені закономірності. Наприклад, масові спроби підбору квитків, атаки через автоматичні скрипти або доступ до API платформ часто відбувається з регулярною періодичністю, особливо при використанні ботнетів. Для виявлення цих закономірностей використовується спектральний аналіз, мета якого – перехід від часового представлення активності до частотного, де можна визначити:

- домінуючі частоти активності, які вказують на регулярні атаки;
- спектральну щільність енергії, яка показує інтенсивність впливу на систему;
- модуляції сигналів, які вказують на зміну стратегії атак.

Вхідними даними можуть виступати часові ряди: кількість звернень досерверу квитків, частоти сканування QR-кодів, кількість відхилень або помилкових спроб входу, мережевий трафік, який пов'язаний з API квитків.

При побудові спектру атак (табл. 1) виконується процедура аналізу, що включає наступні етапи:

1. Збір даних – логування подій на сервері в реальному часі.
2. Попередня обробка – очищення даних, нормування, вибір часового інтервалу (наприклад, 10 секунд, 1 хвилина).
3. Перетворення сигналу (ШПФ) або вейвлет-перетворення.
4. Інтерпретація спектру:

- піки на низьких частотах, що вказують на фонову активність;

- піки на визначених високих частотах – ознаки регулярних автоматизованих атак;
- розширені спектри з високою енергією – можливі DDoS-атаки або скриптова активність.

Таблиця 1

ТИПОВІ СПЕКТРИ АТАК

Тип атаки	Спектральні ознаки	Коментар
Фішинг	Разова активність, нерегулярний сигнал	Спектр слабко визначений, складно передбачуваний
Клонування квитків	Різкі піки при спробі масового входу	Часто співпадає з початком заходу
DDoS-атака	Широкополосний спектр, висока щільність	Миттєве насичення спектру
Бот-атака	Вузькі піки постійної частоти	Періодичні автоматизовані запити

Аналіз цих спектрів дозволяє не тільки визначити загрозу, але й класифікувати її тип, а також прогнозувати поведінку на основі попередніх даних.

Спектральна P-модель захисту за своєю архітектурою представляє собою реактивну математичну систему, яка безперервно спостерігає за системою електронного квитка, аналізує поведінкові та спектральні характеристики запитів, виявляє аномалії, адаптивно реагує на потенційну загрозу.

Загальна архітектура включає наступні компоненти (рис. 1):

1. Модуль збору даних – логує мережеву активність, спроби входу, використання квитків, помилки.
2. Спектральний аналізатор застосовує ШПФ/вейвлет-перетворення до часових рядів.
3. Аналізатор шаблонів – порівнює отриманий спектр з еталонними спектрами відомих атак.
4. Реактивний механізм – ініціює міри захисту в залежності від типу загрози (блокування IP, вимога повторної автентифікації, перехід до обмеженого режиму).
5. Зворотній зв’язок – система навчання, яка корегує модель на основі помилок (наприклад, фальшивопозитивне спрацювання).

```
flowchart LR
A[Дані електронного квитка] --> B[Формування квитка]
B --> C[Спектральне перетворення<br/>(FFT / DWT)]
C --> D[R-вектор<br/>(випадкові параметри)]
D --> E[Захищений контейнер квитка<br/>(QR / PDF417)]

E --> F[Зчитуючий пристрій]
F --> G[Вилучення<br/>спектральних ознак]
G --> H[Зворотня P-модель]

H --> I{Перевірка<br/>дійсності}
I -->|Підтверджений| J[Дозвіл доступу]
I -->|Не підтверджений| K[Відмова / Антифрод]

L[Реєстр еталонних<br/>спектральних ознак]
L --> H
```

Рис. 1. Архітектура спектральної P-моделі захисту електронного квитка

Нехай існує потік подій $x(t)$ – часовий ряд активності системи (наприклад, кілька запитів в секунду). Застосуємо швидке перетворення Фур'є:

$$X(f) = \int_{-\infty}^{\infty} x(t) \cdot e^{-2\pi i f t} dt,$$

де $X(f)$ – спектр сигналу. В той же час $S(f)$ – спектральна щільність відомої атаки. Тоді відхилення можна обчислити як

$$\Delta(f) = |X(f) - S(f)|.$$

Якщо $\max(\Delta(f)) > \theta$, де θ – поріг чутливості, тоді система переходить до режиму реакції. Режим реакції описується системою переходів станів[3]: S_0 – нормальний стан, S_1 – підозра (збір додаткової інформації), S_2 – захист активований (блокування, обмеження), S_3 – поновлення. Перехідна функція R задається у виразі

$$S_{t+1} = R(S_t, \Delta(f), \tau),$$

де $\tau -$ час початку події. Така модель дозволяє адаптувати захист до динаміки атаки.

Для підвищення точності класифікації атак в спектральну Р-модель може бути вбудований класифікатор на основі:

- логістичної регресії;
- градієнтного бустінгу;
- згорткової нейронної мережі (ЗНМ), яка навчена на спектрограмах атак.

Дія алгоритму відбувається за схемою: на вхід моделі надаються спектральні характеристики; класифікатор повертає ймовірність атаки та її тип; система реагує в залежності від ризику і критичності. Тобто, формально маємо гібридну модель, яка поєднує переваги математичної передбачуваності Р-моделі та узагальнюючої здатності нейромереж.

Для перевірки працездатності спектральної Р-моделі була реалізована прототипна система на базі креативних складових: веб-сервіса управління електронними квитками; системи логування подій в реальному часі (на базі **ELK Stack** або **Prometheus+Grafana**); спектрального аналізатора, який написаний на Python з використанням бібліотеки **NumPy** та **SciPy**; нейромережевого класифікатора, який реалізований за допомогою **TensorFlow/Keras**.

Система була розгорнута в тестовому середовищі з імітацією нормального користувацького трафіку і серій цільових атак. Сценарії для моделювання атак надані в таблиці 2. Кожний з таких сценаріїв створював визначену спектральну сигнатуру, що дозволило класифікувати тип атаки до її повного розвитку. Результати моделювання показали, що модель успішно детектує як передбачувані (DDoS, перебір), так і спонтанні атаки (клонування) за рахунок обліку частотних характеристик та адаптивної реактивної логіки.

Таблиця 2

КЛАСИФІКАЦІЯ ТИПУ АТАК

	Тип атаки	Опис
1.	Автоматизований перебір	Ботнет відправляє серію запитів з різними параметрами.
2.	Масове клонування	Багатократне використання одного квитка з різних IP.
3.	DDoS	Експоненційне збільшення кількості запитів до API.
4.	Вброс QR-кодів	Спроба ввести несанкціоновані.

Побудова та моделювання процесів захисту формує множину обмежень та викликів, які повинні бути враховані при застосування Р-моделі. В першу чергу це стосується зашумленості трафіку в умовах великої кількості легітимних користувачів (наприклад, початок масового заходу) – точність моделі знижується. По-друге, при великих навантаженнях може збільшуватись час реакції, що вимагає оптимізації алгоритмів. По-третє, навчання класифікатора вимагає більшої вибірки спектральних представлень атак, що обмежує масштабованість на початкових етапах впровадження.

Для оцінювання ефективності моделі використовувалися наступні метрики: точність виявлення (Precision) – 92,4 %; повнота (Recall) – 89,7 %; F1-міра – 0,91; середній час виявлення атаки – 1,7 секунди; відсоток хибних спрацювань – 4,3 %.

Таким чином, система може бути інтегрована в реальні сервіси електронних квитків при умовах існування системи моніторингу подій, API-інтерфейсу для блокування або призупинення доступу, підтримки потокової обробки даних (наприклад, Kafka або Flink).

Висновки. Розвиток цифрових технологій та зростання популярності електронних квитків для публічних заходів частіше спонтанно, а іноді безперервно, супроводжується збільшенням кіберзагроз. Традиційні засоби захисту вже не можуть впоратися з поліморфною природою атак, що вимагає нових методів моделювання і реагування на них.

У запропонованій статті була розроблена спектральна Р-модель нападу і захисту, яка представлена у вигляді математичного опису взаємодій атакуючого і захисного процесів в часовій та частотні сферах. Основні результати дослідження представлені у вигляді висновків:

- продемонстровано застосування спектрального аналізу (ШПФ) до виявлення і класифікації атак за характерними частотними ознаками;
- побудована математична модель, яка реалізує переходи станів системи в залежності від спектральних характеристик загроз;
- розроблений прототип системи захисту, який включає в себе модулі аналізу, класифікації та адаптивного реагування на загрози;
- проведено тестування моделі на симульованих атаках, що дозволило досягти високих показників точності (F1 = 0,91) та швидкості реакції.

Основною перевагою запропонованого підходу є поєднання високої чутливості до патерн атак з можливістю масштабування і

автоматизації захисту в реальному часі. Таким чином, спектральна P-модель може стати основою для побудови нового класу інтелектуальних систем кібербезпеки, здатних до швидкого навчання, адаптації та автономного прийняття рішень в умовах постійних кіберзагроз.

Бібліографічні посилання

1. Бєгун А. В., Плахтій М. О., Осипова О. І., Урденко О. Г. Огляд ключових технологічних трендів продажу квитків на видовищні заходи/ Моделювання та інформаційні системи в економіці. – К.: КНЕУ. – 2020, № 99, с. 16–31.
2. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: Монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.
3. Жлуктенко В. І., Бєгун А. В. Стохастичні моделі в економіці: Монографія. – К.: КНЕУ, 2005. – 352 с.
4. Yonghua Zhan, Feng Yuan, Rui Shi et al. “Pritkt: A Blockchain-Enhanced Privacy Preserving Electronic Ticket System for IoT Devices.” *Sensors*, 2024, 24(2):496.
5. Maksymenko, Y., Tsurkan V., Dorohyi, Y., Kruk, O. Information security risk assessment based on spectral approach. Collection “Information Technology and Security”, 2015, №3(2), с. 138–146.
6. Jaber, A., et. al. “Graph-based spectral analysis for detecting cyber attacks.” *Proceedings of ARES* (напр. публікація LRE), 2022.
7. Rajalakshmi, N. R., Sathishkumar, V. E., Parameshwari, C. “Cyber-security attack prediction using cognitive spectral clustering technique based on simulated annealing search.” *Applied and Computational Engineering*, 2022.
8. Kotenko, I. V., Saenko, I. B., Lauta O. S., Kriebel, A. M. “Anomaly and Cyber Attack Detection Technique Based on the integration of Fractal Analysis and Machine Learning Methods.” *Informatics and Automation*, 2022, Vol. 21, No. 6, pp. 1328–1358.
9. Raghava Chellu. “Spectral Analysis of Cryptographic Hash Function Using Fourier Techniques.” Journal of Computational Analysis and Applications (JoCAAA), Vol. 30, No. 2, 2022.