

# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0826U000633

**Особливі позначки:** відкрита

**Дата реєстрації:** 23-03-2026

**Статус:** Запланована

**Реквізити наказу МОН / наказу закладу:**



## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Стаматієва Вікторія Вячеславівна

2. Viktoriia V. Stamatieva

**Кваліфікація:**

**Ідентифікатор ORCID ID:** 0000-0003-2721-8985

**Вид дисертації:** доктор філософії

**Аспірантура/Докторантура:** так

**Шифр наукової спеціальності:** 111

**Назва наукової спеціальності:** Математика

**Галузь / галузі знань:** математика та статистика

**Освітньо-наукова програма зі спеціальності:** Математика

**Дата захисту:**

**Спеціальність за освітою:** Математика

**Місце роботи здобувача:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

### III. Відомості про організацію, де відбувся захист

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** PhD 12354

**Повне найменування юридичної особи:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

### IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

**Повне найменування юридичної особи:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

### V. Відомості про дисертацію

**Мова дисертації:** Українська

**Коди тематичних рубрик:** 27.43.15, 27.45.15

**Тема дисертації:**

1. Застосування точкових процесів в узагальненій задачі про дні народження
2. Application of point processes in the generalized birthday problem

**Реферат:**

1. Робота присвячена дослідженню узагальненої задачі про дні народження, яка є важливою проблемою комбінаторної теорії ймовірностей. Розглядаються моменти послідовних надходжень об'єктів одного з  $n$  типів, причому кожен тип вибирається незалежно та рівномірно. Для фіксованого рівня  $r$ , де  $r$  більше або дорівнює одиниці, розглядаються моменти  $r$ -го збігу, тобто такі моменти, коли об'єкт певного типу з'являється в  $r+1$  раз. Основна мета роботи полягає у вивченні асимптотичної поведінки цих моментів за умови, що кількість типів прямує до нескінченності. У дисертації запропоновано єдиний підхід до дослідження цієї задачі, який базується на теорії точкових процесів і їх грубій збіжності. На відміну від класичних підходів, що спираються на твірні або характеристичні функції та потребують складних асимптотичних перетворень, новий підхід дає змогу отримувати граничні теореми більш прозоро та узагальнено. Важливим інструментом є метод пуассонізації, який переводить початкову дискретну модель у

модель неперервного часу і усуває залежність між надходженнями об'єктів різних типів. Після цього здійснюється коректне повернення до вихідної постановки за допомогою депуассонізації. Перший розділ роботи присвячений одновимірним граничним теоремам. У ньому досліджено асимптотичну поведінку процесів моментів  $r$ -го збігу для фіксованого рівня  $r$  у трьох часових шкалах: на початку шкали, у центральній зоні та на правому кінці. Для ранніх збігів доведено збіжність до неоднорідного процесу Пуассона, а для центральної зони — до однорідного процесу Пуассона одичної інтенсивності. Також обґрунтовано процедуру депуассонізації. На основі отриманих результатів знайдено граничні розподіли числових характеристик моделі. Зокрема, встановлено, що нормований момент першого  $r$ -го збігу прямує до розподілу Вейбулла, момент  $k$ -го  $r$ -го збігу має узагальнений гамма-розподіл, а кількість збігів на фіксованому інтервалі часу прямує до розподілу Пуассона. Другий розділ присвячено багатовимірним граничним теоремам і спільній поведінці процесів для різних рівнів  $r$ . У роботі розроблено два підходи до аналізу таких процесів: підхід зі спільним нормуванням і підхід із нормуванням, що залежить від рівня  $r$ . Доведено, що в границі процеси для різних рівнів стають незалежними. Це дає змогу встановити асимптотичну незалежність нормованих моментів перших збігів для різних рівнів, а також отримати явний вигляд щільності розподілу відношення відповідних моментів. У третьому розділі побудовано багаточленний асимптотичний розклад для математичного сподівання моменту першого  $r$ -го збігу. На відміну від відомих класичних одночленних наближень, новий розклад забезпечує значно вищу точність. Для його отримання використано метод Лапласа, який дозволяє аналізувати поведінку підінтегральної функції в околі точки максимуму. Отриманий результат узагальнює відому асимптотику Рамануджана-Ватсона-Кнута на довільний фіксований рівень  $r$ . Проведений чисельний аналіз для випадку  $r=2$  показав істотне зменшення похибки порівняно з класичним наближенням. Практичне значення результатів полягає в можливості їх застосування у криптографії, зокрема для аналізу стійкості геш-функцій до колізій у межах узагальненої атаки днів народження. Крім того, результати можуть бути використані під час статистичного тестування генераторів псевдовипадкових чисел для виявлення прихованих закономірностей у повтореннях.

2. The dissertation is devoted to the study of the generalized birthday problem, an important topic in combinatorial probability theory. It considers the successive arrival times of objects of one of  $n$  types, where each type is chosen independently and with equal probability. For a fixed level  $r$ , the moments of the  $r$ -th coincidence are examined, that is, the times at which an object of a given type appears for the  $r+1$ -st time. The main goal of the work is to investigate the asymptotic behavior of these moments as the number of types tends to infinity. The dissertation proposes a unified approach to the study of this problem based on point process theory and vague convergence. Unlike classical methods relying on generating functions or characteristic functions and requiring complicated asymptotic transformations, the new approach makes it possible to derive limit theorems in a more transparent and general way. An important tool is the method of poissonization, which transforms the original discrete model into a continuous-time model and removes dependence between arrivals of objects of different types. This is followed by a rigorous return to the original setting by means of depoissonization. The first chapter is devoted to one-dimensional limit theorems. It investigates the asymptotic behavior of the processes of  $r$ -th coincidence times for a fixed level  $r$  on three time scales: at the beginning of the scale, in the central zone, and at the right endpoint. For early coincidences, convergence to an inhomogeneous Poisson process is established, while for the central zone, convergence to a homogeneous Poisson process with unit intensity is proved. The depoissonization procedure is also justified. On the basis of these results, the limiting distributions of numerical characteristics of the model are obtained. In particular, it is shown that the normalized time of the first  $r$ -th coincidence converges to a Weibull distribution, the time of the  $r$ -th  $k$ -th coincidence has a generalized gamma distribution, and the number of coincidences on a fixed time interval converges to a Poisson distribution. The second chapter is devoted to multidimensional limit theorems and the joint behavior of the processes for different levels  $r$ . Two approaches to the analysis of such processes are developed: one based on a common normalization and another based on normalization depending on the level  $r$ . It is proved that, in the limit, the processes corresponding to different levels become independent. This makes it possible to establish the asymptotic independence of the normalized times of the first coincidences for different levels, as well as to derive an explicit

form of the density of the distribution of the ratio of the corresponding times. The third chapter develops a polynomial asymptotic expansion for the expectation of the time of the first  $r$ -th coincidence. Unlike the classical one-term approximations known in the literature, the new expansion provides significantly higher accuracy. Its derivation uses Laplace's method, which makes it possible to analyze the behavior of the integrand in a neighborhood of its maximum point. The result generalizes the well-known Ramanujan–Watson–Knuth asymptotic formula to an arbitrary fixed level  $r$ . A numerical analysis for the case  $r=2$  demonstrates a substantial reduction in error compared with the classical approximation. The practical significance of the results lies in their potential applications in cryptography, in particular for analyzing the collision resistance of hash functions within the framework of generalized birthday attacks. In addition, the results may be used in the statistical testing of pseudorandom number generators to detect hidden patterns in repetitions.

**Державний реєстраційний номер ДіР:**

**Пріоритетний напрям розвитку науки і техніки:** Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

**Стратегічний пріоритетний напрям інноваційної діяльності:** Не застосовується

**Підсумки дослідження:** Нове вирішення актуального наукового завдання

**Публікації:**

- Ільєнко А. Б., Стаматієва В. В. Гранична теорема для точкових процесів, пов'язаних з узагальненою задачею про дні народження // Науковий вісник Ужгородського університету. Серія «Математика і інформатика». 2021. Вип. 39, № 2. С. 38–46.
- Стаматієва В. В. Узагальнення асимптотичного розкладу Рамануджана–Ватсона–Кнута // Науковий вісник Ужгородського університету. Серія «Математика і інформатика». 2023. Вип. 43, № 2. С. 52–61.
- Iliencko A., Stamatieva V. Limit theorems in the generalized birthday problem // Bulletin of Taras Shevchenko National University of Kyiv. Series Physics and Mathematics. 2024. No. 2. P. 14–19.
- Стаматієва В. В. Граничні теореми для точкових процесів, пов'язаних із узагальненою задачею про дні народження // XI Всеукраїнська наукова конференція молодих математиків (11–13 травня 2023 р., дистанційно). Київ, 2023. С. 45–46.
- Стаматієва В. В. Узагальнення асимптотичного розкладу Рамануджана–Ватсона–Кнута // XIX Міжнародна наукова конференція ім. академіка М. Кравчука (11–12 жовтня 2023 р., дистанційно). Київ, 2023. С. 183–184.
- Стаматієва В. В. Застосування точкових процесів у граничних теоремах, пов'язаних з узагальненою задачею про дні народження // XII Всеукраїнська наукова конференція молодих математиків (9–11 травня 2024 р., дистанційно). Київ, 2024. С. 46–47.
- Стаматієва В. В. Гранична теорема для багаторівневих точкових процесів в узагальненій задачі про дні народження // XX Міжнародна наукова конференція ім. академіка М. Кравчука (17–20 листопада 2025 р., дистанційно). Київ, 2025. С. 172–173.

**Наукова (науково-технічна) продукція:** методи, теорії, гіпотези

**Соціально-економічна спрямованість:** може бути використано в криптографії для аналізу стійкості геш-функцій до колізій та у статистичному тестуванні генераторів псевдовипадкових чисел

**Охоронні документи на ОПВ:**

**Впровадження результатів дисертації:** Впровадження не планується

**Зв'язок з науковими темами:**

## **VI. Відомості про наукового керівника/керівників (консультанта)**

**Власне Прізвище Ім'я По-батькові:**

1. Ільєнко Андрій Борисович
2. Andrii B. Ilienکو

**Кваліфікація:** к. ф.-м. н., доц., 01.01.05

**Ідентифікатор ORCID ID:** 0000-0003-4828-0788

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

## **VII. Відомості про офіційних опонентів та рецензентів**

**Офіційні опоненти**

**Власне Прізвище Ім'я По-батькові:**

1. Осипчук Михайло Михайлович
2. Muxhailo M. Osypchuk

**Кваліфікація:** д. ф.-м. н., професор, 01.01.05

**Ідентифікатор ORCID ID:** 0000-0001-6100-1654

**Додаткова інформація:**

**Повне найменування юридичної особи:** Карпатський національний університет імені Василя Стефаника

**Код за ЄДРПОУ:** 02125266

**Місцезнаходження:** вул. Шевченка, Івано-Франківськ, 76018, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Власне Прізвище Ім'я По-батькові:**

1. Єлейко Ярослав Іванович

2. Yaroslav I. Yeleiko

**Кваліфікація:** д. ф.-м. н., професор, 01.01.05

**Ідентифікатор ORCID ID:** 0000-0002-2200-8447

**Додаткова інформація:**

**Повне найменування юридичної особи:** Львівський національний університет імені Івана Франка

**Код за ЄДРПОУ:** 02070987

**Місцезнаходження:** вул. Університетська, Львів, 79000, Україна

**Форма власності:** Державна

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:**

**Рецензенти**

**Власне Прізвище Ім'я По-батькові:**

1. Тимошенко Олена Анатоліївна

2. Olena A. Tymoshenko

**Кваліфікація:** к. ф.-м. н., 01.01.05

**Ідентифікатор ORCID ID:** 0000-0003-1885-7275

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

**Власне Прізвище Ім'я По-батькові:**

1. Василик Ольга Іванівна

2. Olha I. Vasylyk

**Кваліфікація:** д. ф.-м. н., доцент, 01.01.05

**Ідентифікатор ORCID ID:** 0000-0002-0880-3751

**Додаткова інформація:**

**Повне найменування юридичної особи:** Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

**Код за ЄДРПОУ:** 02070921

**Місцезнаходження:** проспект Берестейський, Київ, 03056, Україна

