

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

**«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың
XX Халықаралық ғылыми конференциясы = XX Международная
научная конференция студентов и молодых ученых «ǴYLYM JÁNE
BILIM – 2025» = The XX International Scientific Conference for
students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана:
– 3813 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-08-5373-7

**Жинаққа студенттердің, магистранттардың, докторанттардың және жас
ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті
мәселелері бойынша баяндамалары енгізілген.**

**The proceedings are the papers of students, undergraduates, doctoral students and young
researchers on topical issues of natural and technical sciences and humanities. В сборник
вошли доклады студентов, магистрантов, докторантов и молодых ученых по
актуальным вопросам естественно-технических и гуманитарных наук.**

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

| | | | |
|------|--------------------------------------|--|------|
| 518. | Мұрат М.Ж. | Координациялық қосылыстар химиясы бойынша зертханалық курсты әдістемелік қамтамасыз етудегі онлайн материалдардың рөлі | 2188 |
| 519. | Нұралина А.Ж. | Химия сабағында білім алушылардың функционалдық сауаттылығын қалыптастыру | 2192 |
| 520. | Пармантай Қ.Е. | Химияны оқу барысында оқушылардың өзіндік іс-әрекетін олардың интеллектуалдық дамуының құралы ретінде ұйымдастыру | 2197 |
| 521. | Пердеханова А.А. | Дәрілік өсімдіктерді зерттеу барысында студенттердің зерттеушілік құзыреттілігін қалыптастыру | 2202 |
| 522. | Сарсенғалиева А. Н. | Актуальные проблемы в химическом образовании для инженерных специальностей и предлагаемые решения | 2206 |
| 523. | Серікбай А.М. | Мектеп оқушыларының химияға қызығушылығын қалыптастырудың тиімді жолдары | 2209 |
| 524. | Сыздық А.Ф. | Полимерлер мен ауыр мұнай қалдықтарын қолданып, битумның қасиеттерін жақсарту | 2213 |
| 525. | Ташманова Ж.А. | Химияны оқытуда STEM технологиясын пайдалану | 2217 |
| 526. | Тобжанова А.Р. | Мыс(II) галогенидтері – ацетамид – қышқыл жүйесі негізінде координациялық қосылыстар: синтездеу және физика-химиялық қасиеттерін зерттеу | 2222 |
| 527. | Тұрсынәлі Қ. | Қазіргі мектепте «Жаңа заттар мен материалдарды өндіру» элективті курсын оқыту: тәжірибе және нәтижелер | 2227 |
| 528. | Хамит А.Ж. | PASS ONLINE пайдалана отырып N-бензоилпиперидин туындыларының биологиялық белсенділігін болжау | 2232 |
| 529. | Шаихова Ж.Е., Калимолдина Л.М. | Целлюлозалық сорбенттер арқылы шарап материалдарын сорбциялық тазартуды зерттеу | 2237 |
| 530. | Шатлыкова А.Т. | WOLFRAM ALPHA жасанды интеллект құралын химияны оқыту процесінде қолдану мүмкіндіктері | 2241 |
| 531. | Adil K.Y. | Using the getcourse online platform for the unified national test in chemistry | 2245 |
| 532. | Bazhikova Z. | Research of biologically active compounds from plants of the genus ACHILLEA L. | 2249 |

СЕКЦИЯ 4.

МАТЕМАТИКА, МЕХАНИКА И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

ПОДСЕКЦИЯ 4.1 МАТЕМАТИКА

| | | | |
|------|----------------------------------|---|------|
| 204. | Galeeva Dilara Rustemovna | Investigation of the effect of variable viscosity on the velocity of droplet motion in a planar channel | 2253 |
| 205. | Mukhutdinova Aygul Ayratovna | Flow of liquid with variable viscosity in a partially cooled channel with a cavity | 2257 |
| 206. | Melsova Alua | Effective methods of data visualization and statistical analysis | 2259 |
| 207. | Nurgali Nurmadi | Concave function inequalities for accretive dissipative matrices of the τ -measurable operators | 2264 |
| 208. | Onerkhaan A. | The connection of h -amalgamation and joint continuation properties for h - inductive theories | 2268 |
| 209. | Sadvakassov Aidos | On determinantal inequalities of τ -measurable operators | 2266 |
| 210. | Абсаматова Адия Дауыловна | Дискретті жалпыланған Рисс потенциалының өспейтін алмастыруынан туындаған конустардың өзара байланысы | 2272 |
| 211. | Айдос Айбүбі | Нұқсанды дифференциалдық теңдеулердің жалпыланған шешімдері | 2273 |
| 212. | Алдомжарова Томирис Аблайқызы | Шенелмеген коэффициентті бір дифференциалдық оператордың корректілік қасиеті | 2276 |
| 213. | Альжанов Алдияр Маратович | Гармонический анализ на примере моделирования колебаний цен розничных товаров в Республике К азахстан | 2279 |
| 214. | Бағымқызы Бағыжан | Эллис реологиясына негізделген сызықты емес дифференциалдық теңдеулердің аналитикалық және сандық шешімдері | 2284 |

| | | | |
|-----------|------------------------------------|--|------|
| 215. | Бақытжанова Гүлназ Нұрболқызы | Жоғарғы коэффициенті шексіздікте нөлге ұмтылатын үшінші ретті теңдеудің шешімділігі | 2286 |
| 216. | Балагазинова Айым Муратовна | Дискретті салмақты лебег кеңістіктеріндегі дискретті салмақты максималды харди-литтлвуд операторы туралы | 2288 |
| 217. | Гумарова Алия Балкыбековна | Дискретті Рисс потенциалының кейбір қасиеттері | 2289 |
| 218. 5 | Есеналы Алмас | Кездейсоқ графтар теориясының аппроксимациялары | 2292 |
| 219. 6 | Жолдасова Сымбат Жанбулатовна | Модули гладкости и коэффициенты рядов Фурье | 2293 |
| 220. 7 | Исенова А.А., Бағымқызы Б. | Айнымалы коэффициентті сызықты емес бюргер теңдеуі үшін қойылған бастапқы-шеттік есептің шешімділігі | 2296 |
| 221. 8 | Қайратқызы Агнур | Салмақтық Соболев кеңістігінде дербес туындылы дисперсиялық теңдеудің бейсызық тегістігі | 2297 |
| 222. 9 | Серимбетова Акниет Муратқызы | Весовая оценка для одного класса квазилинейных дискретных операторов | 2300 |
| 223. 0 | Смагулова Маржан Толеугазиновна | Үйірткі операторының s сандары | 2302 |
| 224. 1 | Утепбергенова Аида Ерболқызы | Математикалық статистика әдістері негізіндегі ҰБТ нәтижелері мен уақыт арасындағы байланыс | 2304 |

| | | | |
|-----------|-----------------------------|---|------|
| 225. 1 | Халыкберген Надияр | Интерполяционная теорема Марцинкевича-Кальдерона для дискретного пространства Лоренца | 2307 |
| 226. 2 | Чаякова Аяулы Даулетқызы | Математикалық статистика әдістерін жаратылыстану ғылымдарында қолдану | 2309 |

ПОДСЕКЦИЯ 4.2 МЕХАНИКА

| | | | |
|-----------|---|---|------|
| 227. 1 | Galeeva Dilara Rustemovna | Investigation of the effect of variable viscosity on the velocity of droplet motion in a planar channel | 2316 |
| 228. 2 | Mukhutdinova Aygul Ayratovna | Flow of liquid with variable viscosity in a partially cooled channel with a cavity | 2319 |
| 229. 3 | Абдибаттаева Айша Гизатхановна | Математическое моделирование распределение давление поверхность крыла | 2322 |
| 230. 4 | Алпысбаев Нұрәділ Қанатұлы, Махмутов Тілеуқан Қанатұлы | Орта қашықтыққа арналған ұға-ның аэродинамикалық сипатамаларын модельдеу | 2325 |
| 231. 5 | Базарбаев Тамирлан | Конечно-элементный анализ несущей конструкции буровой установки | 2330 |
| 232. 6 | Жанболат Әлихан Қанатұлы | Расчет и анализ аэродинамических характеристик автомобильного кузова | 2334 |
| 233. 7 | Жәлел Әділғазы Әлиұлы | Уран өндіруде жер асты шаймалау әдісін сандық модельдеу | 2337 |

| | | | |
|------------|--|---|------|
| 234. 8 | Жуманбаева Айжан Сериковна | Численный расчет и сравнение моделей турбулентности при моделировании теплообмена в теплообменнике | 2341 |
| 235. 9 | Калиаскер Нұрболат Серікұлы | Қабықша түтікшелі жылу алмастырғыш құбырларындағы бензол мен салқындатқыштың (судың) ағын режимдері мен параметрлерін анықтау | 2345 |
| 236. 0 | Кәлімжан Әлия, Ерзат Мырзахан | Шаңсорғыш роботтың құрылымын жобалау | 2348 |
| 237. 11 | Кенжехан Батырхан Ернатұлы, Тілеубаева Аружан Жомартқызы | Моделирование профиля крыла бпла в зависимости аэродинамических характеристик | 2352 |
| 238. 1 | Маркова Лолита Валерьевна | Компьютерное моделирование падения капли на твердую поверхность в matlab | 2357 |
| 239. 1 | Паклин Леонид Сергеевич | Анализ принципов регулирования режимов резонансных колебаний двухмассной вибрационной машины | 2362 |
| 240. 1 | Рахимбеков Ислам Ерланович | Циклдік координаталық жүйелер үшін Раус әдісін қолдану | 2365 |
| 241. 1 | Русланов Бекнур Русланович | Разработка конструкции багажной аэродромной тележки и расчет на прочность их элементов | 2369 |
| 242. 1 | Тастан Мирас Нұрболатұлы | Өзен арнасын тазалау үшін гидроциклонды сорғылы қондырғылардың параметрлерін есептеу | 2374 |
| 243. 7 | Тілеубаева Аружан Жомартқызы, Кенжехан Батырхан Ернатұлы | Численное моделирование течения жидкости вокруг колеблющейся стенки на программном обеспечении ansys | 2379 |

| | | | |
|-----------|--|---|------|
| 244. 8 | Тулькибаев Чингис Куанышбаевич, Курманова Динара Есентаевна | Влияние граничных условий на теплообменный процесс в расчетах теплообменников | 2382 |
| 245. 9 | Чагин Даниил Михайлович | Влияние ударного взаимодействия на динамику горизонтальной двухмассной ударно-вибрационной площадки | 2384 |

ПОДСЕКЦИЯ 4.3 МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

| | | | |
|-----------|--|--|------|
| 246. | Serikov Samat | Optimization of algorithms for fingerprint search and matching using clustering and approximate nearest neighbor | 2389 |
| 247. | Абат Дулат Ақниетұлы | Ейзенберг моделінің қиратушы толқын типті шешімдері | 2393 |
| 248. 3 | Абдреймова Айгерим Уриякизи | Сандық модельдеу әдістерін қолдана отырып, сызықты емес бөлшек спиндік жүйе үшін жаңа солитон шешімдерін әзірлеу | 2396 |
| 249. 4 | Алайдарова Мөлдір Мамырханқызы | Сандық модельдеуді қолдана отырып, күрделі сызықты емес спиндік жүйе Кауфман-Эккер теңдеуі үшін дәл оптикалық солитон құрылымдарын модельдеу | 2400 |
| 250. 5 | Алтынбек Ж., Алмахан Ер., Асилмаметов Б., Аманжол Ш., Акімхан А. | Числовая угадайка | 2402 |
| 251. 6 | Аскаров А., Әуезхан А., Ғазизханов Е., Баққали А., Сейтенова Б. | Қауіпсіз құпиясөз генераторы | 2404 |
| 252. 7 | Әбілхан Назым Ержанқызы | Есептеу тәсілімен сызықты емес бөлшек спиндік жүйелердің динамикалық теңдеуіне солитондық толқын құрылымын құру | 2407 |

| | | | |
|-----------|---|--|------|
| 253. 8 | Байбатыров Мерхат Маликович | Разработка веб-приложения для учета и сравнения достижений студентов | 2410 |
| 254. 9 | Бақытқан Д., Слямова А., Аширалиева А., Бүркітбай А. | Random модулі туралы | 2412 |
| 255. 0 | Баубек Б., Нурханова А., Альмухамбетова А., Боранов Н., Бегалы Б. | Цезарь шифры туралы | 2415 |
| 256. 1 | Беркімбаев Ислам Жарасқанұлы | Бір солитондық модельдің дисперсиясыз шегі туралы | 2419 |
| 257. 2 | Бисимбаев Рустем Ерланович | Нейросетевое моделирование в композиционных материалах | 2421 |
| 258. 3 | Елеусіз Ақбөбек Мұратбекқызы | Моделирование выбросов и их снижения в ЕНУ | 2426 |
| 259. 1 | Ерғазиева Арина Гайдарқызы | Моделирование динамики развития Капчагайского водохранилища и прогнозирование с использованием искусственного интеллекта | 2428 |
| 260. 5 | Ерғазы Жансая Нұрғазықызы | Жоғары ретті сызықты емес жүйелерді бекітілген уақытта орнықтандыру | 2431 |
| 261. 6 | Жалбасов Абдирахим Шиндаулетович | Көшкіндерді зерттеу әдістері | 2436 |
| 262. 7 | Жанатбек Нұрбақ Нұрланұлы | Использование алгоритмов машинного обучения в диджитал маркетинге | 2441 |
| 263. 8 | Искакова Адина Серікқызы | Вилкоксон критерийін дәріхана бизнесінде машиналық оқыту арқылы қолдану | 2444 |
| 264. 9 | Камал Жайна | DFS алгоритмін қолдану арқылы графтармен жұмыс істеудің тиімді әдістері | 2449 |
| 265. 2 | Кәрғожа Арай Ардаққызы | Сызықты емес спиндік толқындарды модельдеу және динамикалық талдау | 2451 |
| 266. 1 | Кішкене Жұлдыз Асылбекқызы | DEEPFAKE және жасанды интеллект: цифрлық манипуляцияны математикалық модельдеу және анықтау әдістері | 2454 |
| 267. 2 | Мейірбек Құралай Айдынбекқызы | Мейрамхана бизнесіндегі жарнамалық тиімділіктің математикалық моделі | 2459 |
| 268. 3 | Мұқиятұлы Еламан | Бөлшек ретті туындылы Камасса-Холм теңдеуі және оның шешімдері | 2462 |

| | | | |
|-----------|-----------------------------------|---|------|
| 269. 4 | Серік Сабыржан Еркінұлы | Вариациялық есептеу есептерінде функционалдық экстремумды табу үшін жасанды интеллект әдістерін қолдану | 2466 |
| 270. 5 | Сұлтанбеков Жандос Мұсабекұлы | Машиналық оқыту алгоритмдері арқылы жылжымайтын мүлікті бағалау туралы | 2468 |
| 271. 6 | Төлеубек Жібек Ерболқызы | Графтағы циклді іздеу | 2472 |
| 272. 7 | Узахбаев Имангали Хангелди улы | Дамбаларды нақты уақыт мезетінде модельдеу | 2475 |

ПОДСЕКЦИЯ 4.4

МЕТОДИКА ПРЕПОДАВАНИЯ МАТЕМАТИКИ

| | | | |
|------|-------------------------------------|--|------|
| 533. | Абайұлы Есқанат | «Оқыту тиімділігін арттыру үшін практикалық мазмұны бар геометриялық есептерді қолдану» | 2479 |
| 534. | Абдирова Кәмшат Махамбетиярқызы | 7-9 сынып оқушыларының геометрия пәнінде функционалдық сауаттылығын арттырудың маңызы | 2484 |
| 535. | Абдрахманова Жұпар Қабидоллақызы | Математикалық білім берудегі жасанды интеллект | 2488 |
| 536. | Абдуллаева Амина Асанхановна | Математикалық біліктерді қалыптастыруда «тіреу белгілерін» ұтымды қолдану тәсілдері | 2493 |
| 537. | Адібай Аяулым Таубайқызы | Математикада критикалық ойлауды дамытуға арналған креативті әдістер | 2496 |
| 538. | Альбертқызы Бибі | Орта мектепте математиканы гуманитарлық пәндермен байланыстыра оқыту | 2501 |
| 539. | Аманбай Меруерт Маликқызы | Geogebra пайдалану арқылы геометриялық салуларды жүргізу | 2506 |
| 540. | Аманжолова Ажар Дастанқызы | « $(a \pm b)^2$ және $a^2 - b^2$ формулаларының геометриялық мағынасы» | 2510 |
| 541. | Амангельдина Гульдана | Үлгерімі төмен оқушыларға арналған математиканы оқытуда кейбір тәсілдерді тиімді қолдану | 2514 |

| | | | |
|------|--|--|------|
| 542. | Айбосын Гүлзия | Қытайдың математикалық олимпиадалық дайындық жүйесі және Қазақстан үшін оның әдістемелік бейімделуі | 2518 |
| 543. | Аяпбергенова Аяна Женисовна | Интеграция искусства в сферу преподавания математики | 2523 |
| 544. | Әлдиева Жұлдыз Әбдіқадырқызы | Математика пәнін оқытуда дамыта оқыту технологиясын пайдалану | 2525 |
| 545. | Бақыт Ерқанат | Математикалық есептер арқылы оқушылардың | 2531 |
| 546. | Барлыбай Ақниет | Сабақта оқушылардың белсенділігін арттыру үшін дайын сызба және модельдер бойынша тапсырмаларды қолдану | 2533 |
| 547. | Батталов Суңғат | Көпжақтар қималарын мектеп геометрия курсында салу әдістемесі | 2537 |
| 548. | Бахадир Ақтолқын Копжанқызы | Мектеп оқушыларының оқуының тиімділігін арттыру үшін математика сабағында сюжеттік есептерді пайдалану | 2541 |
| 549. | Бекдаулетова Томирис | Математика сабағында әдістемелік нұсқауларды цифрлік форматта қолдану ерекшеліктері | 2545 |
| 550. | Боранбаев Нұрқасым Өскенбайұлы, Сейтжанова Аяулым Маралқызы | Фактор топ және оның дербес жағдайлары | 2550 |
| 551. | Дүйсенбаева Шұғыла Саматқызы | Математика сабағында өмір тәжірибесіне негізделген тапсырмалар | 2554 |
| 552. | Ерболат Аружан | Математика сабағында 5–8 сынып оқушыларына арналған мәтіндік есептерді жүйелі түрде топтастыру және олардың тиімді шешу жолдарын қарастыру | 2557 |
| 553. | Еримбет Дана Каирғалиқызы | Білім сапасын бағалаудың халықаралық зерттеулерінің математикалық сауаттылық тапсырмалары бойынша оқушыларды дайындау | 2560 |
| 554. | Ермекбаев Айдос Елубаевич, Хасенова Тилеужан Сериковна | Методика преподавания математики для студентов обучающихся по программе foundation для подготовки к ент | 2564 |

| | | | | |
|------|--|------------------|---|------|
| 555. | Есентурова Акерке Халеловна | | «Жасанды интеллект: математиканы оқытудың жаңа мүмкіндіктері» | 2567 |
| 556. | Жәрдембек Ғалима | | Мектеп бағдарламасының 8-9 сыныптарындағы математика сабағында цифрлық технологияларды қолдану әдістері | 2570 |
| 557. | Жұмағазы Шұға | | Күрделі математикалық ұғымдарды визуализациялау арқылы оқыту | 2580 |
| 558. | Жұмахан Оралбайқызы | Ақниет | Математикалық диктант: оқушылардың білімін бекітудің тиімді құралы | 2585 |
| 559. | Ибадулла Айғалиқызы | Шұғыла | «Проблемалық оқыту арқылы мектеп оқушыларының математика бойынша зерттеушілік дағдыларын жетілдіру» | 2588 |
| 560. | Икрамов Сағатбекұлы | Ізет | Орта мектепте алгебраны оқыту процесінде тіректік конспектіні пайдалану | 2592 |
| 561. | Иманбетова Мұратқызы | Ақпейіл | Дифференциалдық теңдеулерді мектеп оқушыларына жас ерекшеліктерін ескере отырып оқыту технологиялары | 2596 |
| 562. | Калапбергенова Бауыржановна | Дана | Биология студенттеріне жоғарғы математиканы оқытудың ерекшеліктері | 2599 |
| 563. | Карагизова Ролланқызы, Диана Жасуланқызы | Даурия Даулетжан | Геометрия пәнінде бір есепті әр түрлі әдістермен шешу | 2602 |
| 564. | Каримова Нурболатқызы | Акерке | Сызбалар арқылы математикалық есептерді модельдеу: оқытудағы жұмыс дәптерінің рөлі | 2605 |
| 565. | Кеңес Жеңісбайқызы | Гулден | Мектеп математика курсында теңсіздіктерді оқытудың маңызы | 2606 |
| 566. | Кеңесбай Нұржігітұлы | Бақдәулет | Бұрыш хордасы | 2611 |
| 567. | Қабиден Ерланұлы | Қуаныш | Индивидуальный анализ и рекомендации для учеников с использованием ии | 2611 |
| 568. | Қалдыбек Асылбекұлы | Асылжан | Дифференциалдық теңдеуді грин функциясы әдісімен шешуді оқытудың әдістемесі | 2618 |
| 569. | Құлымбет Төрегелдіқызы | Ақзер | Мектеп оқушыларының функционалдық сауаттылығын дамытудағы pisa | 2622 |
| 570. | Құсайнова Қанатбекқызы | Айдана | Оқушылардың математикалық қабілеттерін диагностикалау мен бағалау әдістері | 2626 |

| | | | | |
|------|--|------------------------|---|------|
| 571. | Марден Қайратқызы | Аяулым | Геометрия сабағындағы топтық жұмыс арқылы оқушылардың белсенділігі мен ойлау қабілетін дамыту | 2630 |
| 572. | Мейманкулова | Сабина | Мектеп геометрия курсындағы салу есептерінің маңыздылығы және факультативтік сабақтардағы қолданылуы | 2634 |
| 573. | Мейрам | Серікболсын | Арифметиканың негізгі теоремасы | 2638 |
| 574. | Мухамедиярова | Ақмарал Анарбекқызы | Сызбалар арқылы математикалық есептерді модельдеу: оқытудағы жұмыс дәптерінің рөлі | 2641 |
| 575. | Мұрат Әділханқызы | Ақбөпе | Декарт координат жүйесін оқыту: тиімді әдістер мен практикалық тапсырмалар | 2644 |
| 576. | Наматулла | Зарина | 7-9 сынып алгебрасындағы “теңдеулер мен теңдеулер жүйесі” бөлімін тапсырмалар арқылы оқыту әдістемесі | 2648 |
| 577. | Несиптаева Арнуровна, Турмухаметова Кайрбековна | Нурай Гульназ | Использование ии в методике преподавания математики | 2652 |
| 578. | Нұржан | Мейір | Интерактивті технологияларды пайдалану арқылы математиканың логикалық негіздерін оқыту | 2655 |
| 579. | Нұржанқызы | Алтынай | 10 сынып геометриясын оқытуда проблемалық оқыту технологиясының элементтерін қолдану және оған мысалдар | 2660 |
| 580. | Орынбасар Шоқанқызы | Жангүл | Көпмүшелер туралы олимпиадалық есептерді шешу әдістері | 2663 |
| 581. | Омирсерик | Султан | Геймификация в обучении математики в школе | 2667 |
| 582. | Сабыров Ердосович | Фархат | Стереометриялық есептерді шешуде жасанды интеллект моделін қолдану | 2671 |
| 583. | Сайлау Оразбайұлы, Мәдіханқызы | Әлия | Оқушыларды олимпиадаға дайындаудағы диофант теңдеулерін шешу әдістері | 2674 |
| 584. | Сафин Мейірханқызы | Ақерке | Сингапурлық оқыту әдістемесі: 7-сыныптың алгебра сабағында «апгрейд 45 минут» моделін қолдану | 2678 |

| | | | | |
|------|--|---------------------|---|------|
| 585. | Сеитханова Медетқызы | Арна | «Алгебра және анализ бастамалары» курсында формулаларды түрлендіру әдістемесі | 2683 |
| 586. | Сексенбай Бекзатқызы | Айтолсын | «Жоғары математиканы оқыту үшін жасаңды интеллект негізінде интерактивті оқу материалдарын жасау» | 2686 |
| 587. | Сарсенбаева Ақниет | | Математика пәнін оқытуда ag және vr технологияларын қолдану | 2690 |
| 588. | Серік Мерей Әсетқызы | | 10-11 сыныптарда қазіргі заманғы цифрлық технологияларды пайдаланып математиканы оқытудың теориялық негіздері | 2696 |
| 589. | Сәбит Сағидолақызы | Елдана | Оқушылардың шығармашылық ойлауын қалыптастыру үшін парадоксалды есептерді пайдалану | 2701 |
| 590. | Смаг Нұрланқызы | Жанерке | Рационал және иррационал енгізілген радикалдар: жіктелуі және әдістемесі | 2704 |
| 591. | Сұлтанғазы Серікқызы | Аружан | 10-сынып математикасы негізінде инклюзивті білім беру теориясы мен практикасы | 2707 |
| 592. | Сыздыкова Жомартовна | Анар | Координаталық әдіс арқылы стереометрия есептерін шешу жолдары | 2712 |
| 593. | Сыздыкова Жомартовна | Анар | Ұбт-ға дайындық: координаталық әдісті тиімді пайдалану | 2715 |
| 594. | Сырымқызы Мөлдір | | Тарихи контекст негізінде қарапайым тригонометриялық теңдеулерді оқыту әдістемесі: теория және тәжірибе | 2719 |
| 595. | Таджекеева Рабаевна, Карлыгаш Муратхановна | Акмарал Оспанова | Математика және тарих пәндері интеграциясының маңызы мен артықшылықтары | 2723 |
| 596. | Тасболат Ержановна | Актоты | Visible thinking в преподавании математики: как сделать мышление учащихся видимым для повышения их понимания и навыков решения задач | 2727 |
| 597. | Тубетова Арманқызы | Малика | «Python негізіндегі интерактивті құрал жасау арқылы ықтималдық есептерін шешуді оқыту» | 2730 |

| | | | | |
|------|-----------------------------------|---------|---|------|
| 598. | Тельманова Жаркыновна | Баян | Математика сабақтарында виртуалды және аралас оқыту | 2735 |
| 599. | Тиллабек Мөлдір | | Мектеп курсында тригонометрияны оқытудың тиімді әдістемесі | 2739 |
| 600. | Тлеухан Баян | | Ою-өрнектер группасының кейбір қасиеттері | 2744 |
| 601. | Турекасым Ибрагимқызы | Жанар | Қысқаша көбейту формулаларының геометриялық мағынасы | 2745 |
| 602. | Тынысбеков Арыстанбек Ардақұлы | | Қолданбалы есептер негізінде комбинаториканы оқыту әдістемесі | 2750 |
| 603. | Хасенова Жандарбековна | Дильназ | Тригонометриялық теңсіздіктерді шешу әдістерінің тиімділігі мен кемшіліктері | 2753 |
| 604. | Хусенбай Алина | | Стереометриялық есептерді шығаруда компьютерлік бағдарламаларды қолдануға мұғалімдерді оқыту әдістемесі | 2757 |
| 605. | Шамелкан Шұғыла | | Әлеуметтік медиа мен жасанды интеллекттің көпмүшеліктерді оқыту мен үйрету тәжірибесіне интеграциясы | 2762 |

ПОДСЕКЦИЯ 4.5

КРИПТОЛОГИЯ

| | | | | |
|------|-------------------------|----------|--|------|
| 606. | Абдуалиев Оразалыұлы | Алмас | Эдвардсдың эллипстік қисықтары | 2765 |
| 607. | Бөрібай Мұқтарұлы | Мирас | Полиалфавиттік Евклидтік шифрды криптоталдау | 2767 |
| 608. | Джубатканов Қуаныш | | Эволюция машинного обучения в криптографии: от теории к постквантовой безопасности | 2769 |
| 609. | Ельтаев Уалиханович | Адильхан | Криптожүйелердегі қайталанбайтын шифрлаудың криптоанализі | 2774 |

| | | | |
|------|---------------------------------------|--|------|
| 610. | Жуматаева Дильназ | Берлекэмп алгоритмі | 2775 |
| 611. | Мұханбетқалиева Назерке Нұрланқызы | Ашық кілтті криптографиялық хаттамаларда гиперэллиптикалық қисықтарды қолдану | 2777 |
| 612. | Өтепберген Ақтілек Дінмұхамбетқызы | Блокчейн жүйелерінде көпфакторлы аутентификацияның тиімділігін арттыру үшін математикалық модельдер мен алгоритмдер. | 2782 |
| 613. | Серікбай Мәншүк Қуанышқызы | Интернет-коммерция үшін заманауи деректерді қорғау протоколдарының тиімділігі | 2787 |
| 614. | Соороков Даулет | Блокчейн технологиясы бойынша зерттеу | 2791 |

СЕКЦИЯ 5

МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

ПОДСЕКЦИЯ 5.1 СОВРЕМЕННЫЕ МЕЖДУНАРОДНЫЕ ПРОЦЕССЫ

| | | | |
|-----------|--------------------------------------|--|------|
| 615. 1 | Абилкасымова Т. Т., Акишева А. Е. | Қазақстанның көпполярлы әлем қалыптастырудағы рөлі: БРИКС және Ғаламдық Оңтүстіктегі ынтымақтастық | 2793 |
| 616. 2 | Амангужинов А. Б. | Начало великого пути: юность и становление Наполеона Бонапарта | 2798 |
| 617. 3 | Алимова М. | Некоторые вопросы взаимного сотрудничества между республиками Кыргызстан и Казахстан: Экономический аспект | 2800 |
| 618. 4 | Ауазбек А.М. | Жасанды интеллект және киберқауіпсіздік: Халықаралық аренадағы жаңа сын-қатерлер. | 2803 |
| 619. 5 | Бегалы Н. Б. | Климаттың өзгеруі және Оңтүстік-Шығыс Азияның экологиялық мәселелері | 2806 |
| 620. 6 | Бейсенғалиева А. Б. | Образ Казахстана в мировых СМИ и международных рейтингах | 2809 |
| 621. 7 | Булатова И. Б., Малик С. Б. | Анализ института рабства в историческом контексте и его отражение в жизни современного общества | 2813 |
| 622. 8 | Гиздетдинов С. Н. | Присутствие Европейского союзав центральной Азии: Конкуренция и перспективы сотрудничества | 2819 |
| 623. 9 | Давлетқан Т.Т. | Незаконная трудовая миграция Казахстанцев в Южную Корею: Проблемы, причины и влияние на взаимоотношения двух стран | 2823 |
| 624. | Ескермесова А. Қ. | Туризм индустриясы: Оңтүстік Шығыс | 2828 |

ПОДСЕКЦИЯ 4.5 КРИПТОЛОГИЯ

ӘОЖ 004.056.55

ЭДВАРДСДЫҢ ЭЛЛИПСТИК ҚИСЫҚТАРЫ

Абдуалиев Алмас Оразалыұлы

almasabdualiev04@gmail.com

Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология

мамандығының 4-курс студенті

Ғылыми жетекшісі – Н. Д. Мархабатов

Бұл мақала Гарольд Эдвардс ұсынған эллиптикалық қисықтардың ерекше түрі – Эдвардс қисықтарына арналған. Мақалада олардың математикалық анықтамасы ($x^2 + y^2 = c^2(1 + dx^2y^2)$) және негізгі ерекшелігі – қарапайым, біртұтас және толық топтық заңы (нүктелерді қосу операциясы) талқыланады. Вейерштрасс формасымен салыстырғандағы артықшылықтарына, атап айтқанда, есептеу тиімділігіне және бүйірлік арна шабуылдарына жоғары төзімділігіне баса назар аударылады. Эдвардс қисықтарының EdDSA сияқты заманауи криптографиялық стандарттар мен цифрлық қолтаңба схемаларындағы маңызды рөлі көрсетіледі. Қорытындыда, бұл қисықтардың эллиптикалық қисық криптографиясы (ECC) үшін тиімділік пен қауіпсіздік тұрғысынан маңызды балама ұсынатындығы атап өтілген.

Кіріспе

Эллиптикалық қисықтар криптографиясы (ECC) қазіргі заманғы ақпараттық қауіпсіздіктің негізгі құрамдас бөліктерінің бірі болып табылады. Олардың негізінде көптеген криптографиялық хаттамалар, соның ішінде сандық қолтаңба схемалары мен кілт алмасу механизмдері құрылған. Эллиптикалық қисықтардың әртүрлі математикалық формалары бар, олардың әрқайсысының өзіндік ерекшеліктері мен артықшылықтары бар. Осындай формалардың бірі – 2007 жылы Гарольд М. Эдвардс ұсынған Эдвардстың эллиптикалық қисықтары. Бұл қисықтар тобы өздерінің қарапайым әрі тиімді топтық заңымен ерекшеленеді, бұл оларды криптографиялық қосымшалар үшін тартымды етеді.

Негізгі бөлім

Сипаттамасы 2-ге тең емес K өрісінде ($\text{char}(K) \neq 2$) анықталған Эдвардстың эллипстік қисығы келесі түрдегі теңдеумен беріледі:

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

мұндағы c және d - K өрісінің тұрақтылары, $c \neq 0$ және $d \neq 0$. Жиі қолданылатын, жеңілдетілген жағдай $c = 1$ болып табылады, бұл кезде теңдеу келесі түрге келеді:

$$x^2 + y^2 = 1 + dx^2y^2$$

Бұл жағдайда, қисықтың анықталуы үшін d элементі K өрісінде квадрат болмауы тиіс. Эдвардс қисықтары Вейерштрасс формасындағы эллиптикалық қисықтарға бирационалды эквивалентті, яғни олардың арасында өзара бірмәнді сәйкестік орнатуға болады (кейбір ерекше нүктелерді есептемегенде).

Топтық заң:

Эдвардс қисығының ең маңызды қасиеттерінің бірі – оның нүктелерінде анықталған топтық операцияның (қосудың) қарапайымдылығы мен толықтығы. Қисықтағы нүктелер жиыны осы қосу операциясы бойынша Абель тобын құрайды.

1. Бейтарап элемент (Нөлдік элемент): Топтың бейтарап элементі болып $O = (0, c)$ нүктесі табылады (жеңілдетілген $c=1$ жағдайында $O = (0, 1)$).
2. Кері элемент: $P = (x, y)$ нүктесіне кері элемент $-P = (-x, y)$ болады.
3. Нүктелерді қосу: Эдвардс қисығындағы $P_1 = (x_1, y_1)$ және $P_2 = (x_2, y_2)$ нүктелерінің қосындысы $P_3 = (x_3, y_3)$ келесі формулалармен анықталады:

$$x_3 = (x_1y_2 + y_1x_2) / (c(1 + dx_1x_2y_1y_2))$$

$$y_3 = (y_1y_2 - x_1x_2) / (c(1 - dx_1x_2y_1y_2))$$

Бұл формулалар "біртұтас" (unified) болып табылады, яғни олар $P_1 \neq \pm P_2$ болғанда нүктелерді қосу үшін де, $P_1 = P_2$ болғанда нүктені екі еселеу (doubling) үшін де жарамды. Бұл Вейерштрасс формасынан айырмашылығы, онда нүктені қосу мен екі еселеу үшін әртүрлі формулалар қолданылады және шексіздіктегі нүктемен байланысты ерекше жағдайларды қарастыру қажет.

Эдвардс қисықтарының қосу заңы "толық" (complete) болып саналады, яғни ол топтың бейтарап элементі мен кері элементтерден басқа кез келген екі нүктені қосу үшін ерекше жағдайларсыз қолданыла береді. Бұл қасиет, әсіресе, қисықтың Twisted Edwards деп аталатын жалпыланған түрінде айқын көрінеді ($ax^2 + y^2 = 1 + dx^2y^2$).

Артықшылықтары:

Эдвардс қисықтарының Вейерштрасс формасындағы қисықтармен салыстырғанда бірқатар артықшылықтары бар:

1. Есептеу тиімділігі: Біріздендірілген және толық қосу заңы нүктелік арифметиканы жеделдетуге мүмкіндік береді. Әрбір нүктені қосу операциясы аз элементар амалдарды талап етуі мүмкін.
2. Бүйірлік арна шабуылдарына төзімділік: Криптографиялық жүйелерде нүктені қосу мен екі еселеу операцияларының орындалу уақытындағы айырмашылықты пайдаланып, құпия кілт туралы ақпарат алуға тырысатын бүйірлік арна шабуылдары (мысалы, timing attack) бар. Эдвардс қисықтарындағы біріздендірілген қосу формуласы мұндай шабуылдарға қарсы тұруды жеңілдетеді, себебі қосу мен екі еселеу операциялары бірдей алгоритммен орындалады.
3. Іске асырудың қарапайымдылығы: Толық қосу заңы ерекше жағдайларды өңдеу қажеттілігін азайтады, бұл криптографиялық кітапханаларды іске асыруды жеңілдетеді және қателіктердің пайда болу ықтималдығын төмендетеді.

Қолданылуы:

Эдвардс қисықтары, әсіресе олардың Twisted Edwards түрлері, заманауи эллиптикалық қисық криптографиясында кеңінен қолданыс табуда. Олардың негізінде жоғары өнімділік пен қауіпсіздікті талап ететін криптографиялық схемалар құрылған. Мысалы:

EdDSA (Edwards-curve Digital Signature Algorithm): Бұл Schnorr қолтаңбасының Эдвардс қисықтарына бейімделген нұсқасы. EdDSA өзінің жылдамдығымен және бүйірлік арна шабуылдарына жоғары төзімділігімен танымал. Curve25519 және Ed448 сияқты танымал қисықтар көбінесе Эдвардс немесе Монтгомери формасында (олар бір-бірімен тығыз байланысты) іске асырылады.

Кілт алмасу хаттамалары: Эдвардс қисықтары Диффи-Хеллман кілт алмасу хаттамасының эллиптикалық қисықтарға негізделген нұсқаларында (ECDH) қолданылуы мүмкін.

Қорытынды

Мақалада Эдвардс қисықтарының жалпы анықтамасы негізгі ерекшеліктері талқыланды. Вейерштрасс формасымен салыстырғандағы артықшылықтары, есептеу тиімділігі мен бүйірлік арна шабуылдарына жоғары төзімділігіне баса назар аударылды. Эдвардс қисықтарының EdDSA секілді заманауи криптографиялық стандарттар мен цифрлық қолтаңба схемаларындағы маңызды рөлі көрсетілді. Эдвардстың эллиптикалық қисықтары эллиптикалық қисықтар теориясының маңызды бір тармағын құрайды. Олардың қарапайым, біріздендірілген және толық топтық заңы криптографиялық қосымшалар үшін елеулі артықшылықтар береді, соның ішінде есептеу тиімділігін арттыру және бүйірлік арна шабуылдарына қарсы қорғанысты күшейту. Осы қасиеттерінің арқасында Эдвардс қисықтары заманауи криптографиялық стандарттар мен жүйелерде маңызды орын алады.

Қолданылған әдебиеттер тізімі:

1. Edwards, H. M. (2007). A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3), 393–422.
2. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards curves. In *Progress in Cryptology—AFRICACRYPT 2008* (pp. 389–405). Springer Berlin Heidelberg.
3. Bernstein, D. J., & Lange, T. (2007). Faster addition and doubling on elliptic curves. In *Advances in Cryptology—ASIACRYPT 2007* (pp. 29–50). Springer Berlin Heidelberg.
4. Josefsson, S., & Liusvaara, I. (2017). Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032. Internet Engineering Task Force (IETF).
5. Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography* (2nd ed.). CRC Press.

ӘОЖ 004.056.55

ПОЛИАЛФАВИТТІК ЕВКЛИТІК ШИФРДЫ КРИПТОЛДАУ

Бөрібай Мирас Мұқтарұлы

boribay.m@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Мархабатов Н. Д.

Қазіргі заманғы ақпараттық қауіпсіздік саласында криптографиялық әдістердің маңыздылығы артып келеді. Полиалфавиттік Евклидтік шифр – бұл жаңа математикалық тәсілдерге негізделген шифрлау әдісі, оның ерекшелігі бірнеше алфавиттік ауысуларды қолдануында. Бұл диссертацияда полиалфавиттік Евклидтік шифрдың құрылымы, оның математикалық негіздері, беріктігі мен әлсіз жақтары қарастырылады.

Криптография – ақпаратты қорғаудың негізгі құралы болып табылады. Полиалфавиттік шифрлар ақпаратты қорғауда маңызды рөл атқарады, себебі олар қарапайым ауыстыру шифрларына қарағанда күрделірек құрылымға ие. Евклидтік алгоритм негізінде құрылған шифр ақпаратты сенімді қорғауға мүмкіндік береді. Ақпараттық қауіпсіздік қазіргі заманғы цифрлық технологиялардың ажырамас бөлігі болып табылады. Құпия мәліметтерді қорғау үшін әртүрлі криптографиялық әдістер қолданылады, олардың ішінде шифрлау әдістері ерекше орын алады. Криптографияның негізгі бағыттарының бірі — полиалфавиттік шифрлар, олардың арасында Евклидтік шифр ерекше зерттеуді қажет етеді. Бұл жұмыста полиалфавиттік Евклидтік шифрды криптоанализдеу мәселелері қарастырылады.