ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM 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, докоранттардың 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 имолодыхученых 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

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 коэфициентті бір дифференциалдық операторды 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., Багымкызы 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 Мураткызы	Весовая оценка для одного класса квазилинейных дискретных операторов	2300
223.0	Смагулова Маржан Толеугазиновна	Үйірткі операторының s сандары	2302
224.1	Утепбергенова Аида Ерболкызы	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 ұұа-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 програмном 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	Optimazation 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	Беркімбай 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	Ергазиева 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 Каиргалиқызы	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 Ақниет Оралбайқызы	Математикалық диктант: оқушылардың білімін бекітудің тиімді құралы	2585
559.	Ибадулла Шұғыла Айғалиқызы	«Проблемалық оқыту арқылы мектеп оқушыларының математика бойынша зерттеушілік дағдыларын жетілдіру»	2588
560.	Икрамов Ізет Сағатбекұлы	Орта мектепте алгебраны оқыту процесінде тіректік конспектіні пайдалану	2592
561.	Иманбетова Ақпейіл Мұратқызы	Дифференциалдық теңдеулерді мектеп оқушыларына жас ерекшеліктерін ескере отырып оқыту технологиялары	2596
562.	Калапбергенова Дана Бауыржановна	Биология студенттеріне жоғарғы математиканы оқытудың ерекшеліктері	2599
563.	Карагизова Даурия Ролланқызы, Даулетжан Диана Жасуланқызы	Геометрия пәнінде бір есепті әр түрлі әдістермен шешу	2602
564.	Каримова Акерке Нурболаткызы	Сызбалар арқылы математикалық есептерді модельдеу: оқытудағы жұмыс дәптерінің рөлі	2605
565.	Кеңес Гулден Жеңісбайқызы	Мектеп математика курсында теңсіздіктерді оқытудың маңызы	2606
566.	Кеңесбай Бақдәулет Нұржігітұлы	Бұрыш хордасы	2611
567.	Қабиден Қуаныш Ерланұлы	Индивидуальный анализ и рекомендации для учеников с использованием ии	2611
568.	Қалдыбек Асылжан Асылбекұлы	Дифференциалдық теңдеуді грин функциясы әдісімен шешуді оқытудың әдістемесі	2618
569.	Құлымбет Ақзер Төрегелдіқызы	Мектеп оқушыларының функционалдық сауаттылығын дамытудағы pisa	2622
570.	Құсайнова Айдана Қанатбекқызы	Оқушылардың математикалық қабілеттерін диагностикалау мен бағалау әдістері	2626

571.	Марден Аяулым Қайратқызы	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 Ақбөпе Әділханқызы	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 Нурай Арнуровна, Турмухаметова Гульназ Кайрбековна	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 Жангүл Шоқанқызы	Көпмүшелер туралы олимпиадалық есептерді шешу әдістері	2663
581.	Омирсерик Султан	Геймификация в обучении математики в школе	2667
582.	Сабыров Фархат Ердосович	Стереометриялық есептерді шешуде жасанды интеллект моделін қолдану	2671
583.	Сайлау Ерлан Оразбайұлы, Мәдіханқызы Әлия	Оқушыларды олимпиадаға дайындаудағы диофант теңдеулерін шешу әдістері	2674
584.	Сафин Ақерке Мейірханқызы	Сингапурлық оқыту әдістемесі: 7-сыныптың алгебра сабағында «апгрейд 45 минут» моделін қолдану	2678

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

598.	Тельманова Баян Жаркыновна	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 Жанар Ибрагимқызы	Қысқаша көбейту формулаларының геометриялық мағынасы	2745
602.	Тынысбеков Арыстанбек Ардақұлы	Қолданбалы есептер негізінде комбинаториканы оқыту әдістемесі	2750
603.	Хасенова Дильназ Жандарбековна	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 интелекттің көпмүшеліктерді оқыту мен үйрету тәжірибесіне интеграциясы	2762

ПОДСЕКЦИЯ 4.5

КРИПТОЛОГИЯ

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

СЕКЦИЯ 5

МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

ПОДСЕКЦИЯ 5.1 СОВРЕМЕННЫЕ МЕЖДУНАРОДНЫЕ ПРОЦЕССЫ

УДК 004.056.55

ЭВОЛЮЦИЯ МАШИННОГО ОБУЧЕНИЯ В КРИПТОГРАФИИ: ОТ ТЕОРИИ К ПОСТКВАНТОВОЙ БЕЗОПАСНОСТИ

Джубатканов Қуаныш
kuanysh595@gmail.com
ЕНУ им. Л. Н. Гумилева, докторант кафедры Криптологии, Астана, Казахстан
Научный руководитель – Танирбергенов А.Ж.

Аннотация

Интеграция машинного обучения (ML) в сферу криптографии стала значительным вектором научного развития в последние десятилетия. Использование интеллектуальных алгоритмов не только усилило существующие криптографические методы, но и породило новые подходы к анализу безопасности, защите конфиденциальности и выявлению уязвимостей. Данная статья представляет обзор ключевых этапов развития машинного обучения в криптографии с 1995 по 2025 год, включая нейрокриптографию, гомоморфное шифрование, автоматизированный криптоанализ и постквантовые исследования. Особое внимание уделено как достижениям, так и вызовам, связанным с этическими аспектами, устойчивостью к атакам и вычислительной эффективностью. Работа направлена на формирование целостного представления о текущем состоянии и будущем потенциале этой междисциплинарной области.

Ключевые слова: машинное обучение; криптография; нейрокриптография; гомоморфное шифрование; постквантовая криптография; приватность данных; криптоанализ; федеративное обучение; трансформеры; информационная безопасность.

Введение

В условиях стремительной цифровизации общества защита информации приобретает всё более критическое значение. Практически все сферы человеческой деятельности — от финансов и медицины до обороны и государственного управления — зависят от надёжности систем хранения и передачи данных. На протяжении десятилетий криптография оставалась основой обеспечения информационной безопасности, опираясь на математическую строгость, теорию чисел и устойчивость алгоритмов к атакам с высокой вычислительной сложностью. Однако появление и развитие новых вычислительных парадигм, в частности, машинного обучения (ML), стало одним из самых значимых факторов, влияющих на трансформацию подходов к криптографической защите.

Машинное обучение — это область искусственного интеллекта, которая занимается разработкой алгоритмов, способных обучаться на данных и принимать решения без явного программирования. Первоначально ML использовалось в задачах классификации, распознавания образов и прогнозирования. Однако по мере увеличения доступных вычислительных ресурсов и роста объёмов данных машинное обучение начало проникать в более специализированные и критически важные области, включая кибербезопасность и криптографию.

Интеграция ML в криптографию происходит по двум направлениям — защитному и атакующему. С одной стороны, машинное обучение активно применяется для укрепления систем безопасности: создание устойчивых к атаке классификаторов вредоносного ПО, разработка защищённых вычислений на зашифрованных данных, анализ поведения систем и автоматическая генерация криптографических протоколов. С другой стороны, ML также

демонстрирует высокую эффективность в области криптоанализа: автоматическое восстановление ключей, анализ утечек через побочные каналы, атаки на шифры с помощью нейросетей и трансформеров — всё это стало возможным благодаря способности ML находить сложные закономерности и эксплуатировать уязвимости, неочевидные для традиционных методов.

Особенно интересен тот факт, что применение ML не ограничивается классической криптографией. В условиях приближающейся угрозы квантовых вычислений активно развиваются направления постквантовой криптографии, в которых также находят применение методы машинного обучения. Новые архитектуры, такие как трансформеры, используются для анализа решёток и других устойчивых к квантовым атакам структур. Наряду с этим, развитие гомоморфного шифрования и федеративного обучения позволяет строить приватные системы машинного обучения, не раскрывающие данные ни пользователю, ни серверу.

Таким образом, взаимодействие ML и криптографии сегодня представляет собой не просто симбиоз, а активное поле научной конкуренции и сотрудничества. Оно формирует новые подходы к проектированию систем безопасности, вносит вызовы в традиционные криптографические допущения и требует пересмотра этических и нормативных рамок. Данная статья посвящена исследованию этой взаимосвязи в ретроспективе и настоящем: от первых теоретических разработок в конце XX века до современных достижений в области защищённых вычислений и постквантового криптоанализа. Кроме того, рассматриваются ключевые вызовы, сдерживающие повсеместное внедрение таких технологий, включая вычислительную сложность, устойчивость к атакующим примерам и риски двойного использования.

Ранние этапы развития: 1995–2010

Период с 1995 по 2010 год можно охарактеризовать как зарождение интереса к интеграции машинного обучения в криптографию. В эти годы формировалась теоретическая база ML, развивались методы нейросетевого моделирования, статистического анализа и устойчивого обучения, что постепенно подготовило почву для применения этих подходов в области защиты информации.

В конце 1990-х годов машинное обучение сосредотачивалось на разработке интерпретируемых и устойчивых моделей. Особое внимание уделялось обучению с шумом, обобщающей способности нейронных сетей и созданию гибридных систем, сочетающих обучение и логический вывод [6][7][8]. Эти идеи оказались важными для будущего использования в криптографических задачах, особенно там, где требовалась обработка неполных или зашумлённых данных.

С начала 2000-х годов появляются первые работы, где машинное обучение начинает использоваться непосредственно в криптографии. Наиболее заметным направлением становится нейрокриптография, основанная на Tree Parity Machines (TPM) — архитектуре нейронной сети, применяемой для безопасного обмена ключами без предварительной договорённости [1][2]. Синхронизация таких сетей происходила путём обмена выходами на общих входных данных, в результате чего обе стороны приходили к идентичному весовому вектору, который становился общим секретным ключом.

Дополнительную безопасность обеспечивала модификация с синхронизацией по запросам, предложенная позже [3], затруднявшая работу потенциальных атакующих. Это стало важным шагом к созданию дешёвых и надёжных протоколов для устройств с ограниченными вычислительными возможностями.

Параллельно развивались и другие направления. В частности, в рамках статистической криптографии были предложены модели, основанные на квантово-вдохновлённой статистике, например, модель Фишера–Шрёдингера, позволяющая реализовать адаптивное шифрование [4]. Кроме того, исследования в области устойчивости обучения при наличии ошибок, такие как работа A. Blum и коллег [5], укрепили позиции ML как инструмента для создания и анализа криптографических примитивов, базирующихся на функции паритета.

Таким образом, период 1995–2010 стал этапом теоретического сближения двух областей — машинного обучения и криптографии. Были предложены первые реальные криптографические протоколы на базе нейросетей, а также продемонстрирована применимость ML для анализа и моделирования сложных криптографических систем.

Развитие и применение: 2010–2020

В период с 2010 по 2020 год машинное обучение вышло на качественно новый уровень: бурное развитие нейросетевых архитектур, особенно глубокого обучения (deep learning), привело к резкому росту интереса к ML в контексте кибербезопасности и криптографии. Исследователи стали использовать интеллектуальные алгоритмы не только как вспомогательный инструмент анализа, но и как центральный элемент в автоматизации криптографических задач, защите конфиденциальности и выявлении угроз.

Одним из наиболее значимых достижений стало развитие методов privacy-preserving machine learning (PPML) — защищённого машинного обучения, позволяющего проводить анализ данных, не раскрывая их содержимого. На передний план вышло гомоморфное шифрование (Homomorphic Encryption, HE), с помощью которого стало возможно выполнять математические операции над зашифрованными данными. Это позволило обучать модели машинного обучения, не нарушая приватность пользователей [9][11].

Так, например, были разработаны алгоритмы для наивных байесовских классификаторов и случайных лесов, способных работать непосредственно на зашифрованных данных, с результатами, приближающимися по точности к обычным моделям [9]. Несмотря на высокие вычислительные затраты, эти методы открыли путь к безопасной аналитике в чувствительных сферах, таких как медицина и финансы.

Другим важным направлением стало применение ML в автоматизированном криптоанализе. В работе D. Hosfelt [10] была представлена система на основе машинного обучения для распознавания и классификации криптографических алгоритмов в бинарных программах. Модели обучались на выборках исполняемых файлов, содержащих реализацию таких шифров, как RSA, AES и DES. Система продемонстрировала высокую точность в определении используемых алгоритмов и их параметров, что имеет важное значение для анализа вредоносного ПО и обратной инженерии.

Особое внимание в этот период стало уделяться применению ML в задачах обнаружения киберугроз, в частности, рансомвар-атак. Исследования показали, что поведенческие модели, обученные на признаках вредоносной активности (изменения файлов, доступ к системным ресурсам, аномальные процессы), способны с высокой точностью выявлять атаки и блокировать их на ранней стадии [12]. В таких решениях широко применялись методы глубинного обучения, в том числе рекуррентные сети (LSTM), а также adversarial training — обучение моделей устойчивости к попыткам обхода детекторов.

Наконец, в этот период началась активная разработка протоколов на стыке криптографии и ML, сочетающих преимущества обеих областей. Это выразилось в появлении гибридных подходов, где классические криптографические методы (например, шифрование)

дополнялись ML-алгоритмами, обеспечивающими адаптацию, настройку параметров безопасности и управление ключами в реальном времени.

Таким образом, десятилетие 2010–2020 стало эпохой практической реализации идей, заложенных ранее. Машинное обучение укрепило свои позиции как неотъемлемый компонент современного криптографического инструментария: от приватного анализа данных до автоматического взлома уязвимых реализаций шифров.

Современные достижения и вызовы: 2020–2025

Последние годы ознаменованы качественным скачком в интеграции машинного обучения в криптографию. С 2020 года область переживает период стремительной эволюции: на фоне бурного роста мощностей ИИ, появления квантовых угроз и масштабной цифровизации (в том числе в IoT и здравоохранении) машинное обучение стало неотъемлемым компонентом как оборонительных, так и атакующих криптографических решений.

Одним из ключевых направлений стало применение ML в области постквантовой криптографии (Post-Quantum Cryptography, PQC). Примером служит работа SALSA (Secure Algorithm Learning for Sieve Approximation), в которой трансформеры (архитектуры, широко применяемые в NLP) использовались для криптоанализа задач на основе решёток (Learning With Errors, LWE) — одного из базовых элементов PQC [13]. Трансформер-модели обучались на больших выборках криптографических задач и продемонстрировали способность приближённо решать их с эффективностью, недоступной традиционным алгоритмам.

Продолжением этой идеи стала разработка SALSA FRESCA, в которой использовались угловые встраивания (angular embeddings), предварительное обучение и специализированные архитектуры для повышения эффективности атак на LWE-проблемы с большой размерностью [16]. Это стало тревожным сигналом для разработчиков постквантовых алгоритмов: ML способен выявлять слабые места даже в наиболее защищённых конструкциях.

В то же время активно развивались методы приватного и распределённого обучения. Системы вроде GuardML [15] предложили эффективные решения на основе гибридного гомоморфного шифрования (Hybrid Homomorphic Encryption), совмещающего полное и частичное шифрование для оптимального баланса между производительностью и безопасностью. Такие подходы позволяют проводить ML-обработку зашифрованных данных прямо на клиентских устройствах или в облаке, не раскрывая ни данных, ни модели.

Параллельно усилился интерес к федеративному обучению, при котором данные остаются на стороне пользователя, а обучение происходит распределённо. Это особенно актуально для мобильных устройств, медицинских датчиков и промышленных IoT-систем, где конфиденциальность и вычислительные ограничения критичны.

С другой стороны, ML всё чаще используется в качестве инструмента криптоанализа. Работы вроде CRYPTO-MINE [14] показали, что нейросети могут оценивать взаимную информацию между шифротекстом и открытым текстом, тем самым обнаруживая утечки, ранее недоступные классическим статистическим методам. Также были предложены гибридные подходы, сочетающие градиентный спуск и симуляцию криптографических атак [17], демонстрирующие высокую эффективность при взломе плохо реализованных алгоритмов.

На фоне этих достижений всё острее встаёт вопрос двойного назначения подобных технологий. Один и тот же ML-инструмент может быть использован как для усиления защиты,

так и для проведения атак. Это требует особого внимания к этическим и нормативным вопросам, включая регуляцию применения ИИ в сфере безопасности.

Таким образом, период 2020–2025 — это время практической реализации, масштабирования и пересмотра допущений. ML перестаёт быть вспомогательным инструментом и становится полноправным участником криптографического процесса, способным как создавать, так и разрушать системы безопасности. Основные задачи будущего — обеспечить масштабируемость, устойчивость к атакующим примерам, и самое главное — ответственное использование таких технологий.

Заключение

Интеграция машинного обучения в криптографию представляет собой одно из наиболее динамично развивающихся направлений современной информационной безопасности. От первых теоретических моделей, сформированных в 1990-х годах, до современных реализаций в постквантовых сценариях, мы наблюдаем последовательное и логичное сближение двух ранее самостоятельных дисциплин.

В начале пути машинное обучение использовалось преимущественно как метод анализа и обработки сложных или зашумлённых данных, закладывая основы будущей интеграции в криптографические системы. В 2000-х годах появились первые практические реализации нейрокриптографии, продемонстрировавшие возможность безопасного обмена ключами с использованием свойств нейросетей. Следующее десятилетие стало временем масштабного внедрения ML в практику: от гомоморфного обучения на зашифрованных данных до автоматического распознавания криптоалгоритмов и защиты от вредоносного ПО.

Современный этап (2020–2025) знаменует собой выход машинного обучения на уровень системообразующего элемента в криптографии. Такие технологии, как трансформеры, федеративное обучение, гибридные методы шифрования и нейронный криптоанализ, радикально меняют как архитектуру защищённых систем, так и сам подход к понятию «безопасность».

Однако наряду с успехами остаются и вызовы. Среди них — высокая вычислительная сложность, уязвимость моделей к атакующим воздействиям, проблемы масштабируемости и, самое главное, этические и нормативные риски, связанные с двойственным использованием ML-инструментов. Один и тот же алгоритм может быть использован как для защиты, так и для атаки, что требует взвешенного подхода и регуляторного надзора.

Таким образом, будущее криптографии невозможно представить без тесного взаимодействия с машинным обучением. Эта взаимосвязь должна строиться на принципах ответственности, прозрачности и научной обоснованности. Только в этом случае мы сможем использовать потенциал ML во благо информационной безопасности, а не во вред.

Список литературы:

1. Kinzel W., Kanter I. Neural cryptography.
2. Rosen-Zvi M., Klein E., Kanter I., Kinzel W. Mutual learning in a tree parity machine and its application to cryptography. *arXiv:cond-mat/0209234v1*
3. Ruttor A., Kinzel W., Kanter I. Neural cryptography with queries.
4. Venkatesan R. C. Statistical cryptography using a Fisher–Schrödinger model.
5. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model.
6. Weiss S. M., Indurkhya N. Rule-based machine learning methods for functional prediction.
7. Sporre M. Unrealizable learning in feedforward neural networks.

8. Giraud-Carrier C. G., Martinez T. R. An integrated framework for learning and reasoning.
9. Aslett L. J. M., Esperança P. M., Holmes C. C. Encrypted statistical machine learning: New privacy preserving methods.
10. Hosfelt D. Automated detection and classification of cryptographic algorithms in binary programs through machine learning.
11. Aslett L. J. M., Esperança P. M., Holmes C. C. A review of homomorphic encryption and software tools for encrypted statistical machine learning.
12. Yang C.-Y., Sahita R. Towards a resilient machine learning classifier: A case study of ransomware detection.
13. Wenger E., Chen M., Charton F., Lauter K. SALSA: Attacking lattice cryptography with transformers.
14. Kim B. D., Vasudevan V. A., Woo J., et al. CRYPTO-MINE: Cryptanalysis via mutual information neural estimation.
15. Frimpong E., Nguyen K., Budzys M., et al. GuardML: Efficient privacy-preserving ML services through hybrid homomorphic encryption.
16. Stevens S., Wenger E., Li C., et al. SALSA FRESCA: Angular embeddings and pre-training for ML attacks on learning with errors.
17. Shafran A., Malach E., Ristenpart T., Segev G., Tessaro S. Is ML-based cryptanalysis inherently limited?

ӘОЖ 004.056.55

Криптожүйелердегі қайталанбайтын шифрлаудың криптоанализі

Ельтаев Адильхан Уалиханович
Adilkhaneltaev05@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Мархабатов Н. Д.

Қазіргі ақпараттық қауіпсіздік саласында криптографиялық жүйелердің маңыздылығы артып келеді. Ақпарат алмасу барысында деректердің құпиялығын сақтау үшін әртүрлі шифрлау әдістері қолданылады. Соның ішінде қайталанбайтын шифрлау тәсілдері ерекше орын алады. Бұл әдістердің негізгі ерекшелігі – бірегей кілттер немесе кездейсоқ түрде өзгеретін шифрлау алгоритмдерін қолдануында.

Криптоанализ қайталанбайтын шифрлау жүйелерінің беріктігін бағалауға және олардың әлсіз тұстарын анықтауға бағытталған. Қайталанбайтын шифрлау әдістерін талдау барысында шифрланған мәтіннің кездейсоқтық дәрежесін бағалау үшін энтропия ұғымы қолданылады. Егер $H(C)$ – шифрланған мәтіннің энтропиясы, ал $H(K)$ – қолданылған кілттің энтропиясы болса, онда мінсіз шифрлау жағдайында:

$$H(C|K) = H(M)$$

мұнда M – ашық мәтін. Бұл теңдік шифрланған деректердің толықтай қорғалғанын және оларды кілтсіз ашу мүмкін еместігін білдіреді.

Криптоанализ әдістері жиілік талдау, белгілі ашық мәтін шабуылдары және сызықтық криптоанализ сияқты тәсілдерді қамтиды. Қайталанбайтын шифрлау әдістеріне қарсы шабуыл жасау кезінде негізгі қиындық – кілттің өзгермелілігі мен жоғары энтропия деңгейі болып табылады. Бұл факторлар криптожүйенің беріктігін арттырады.

Қорыта айтқанда, қайталанбайтын шифрлау әдістерін зерттеу көрсеткендей, мұндай тәсілдер деректерді қорғаудың жоғары деңгейін қамтамасыз етеді. Дегенмен, олардың практикалық