

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

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

**Студенттер мен жас ғалымдардың  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»  
XIX Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XX Международной научной конференции  
студентов и молодых ученых  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS  
of the XX International Scientific Conference  
for students and young scholars  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**2025  
Астана**

УДК 001(06)  
ББК 72я631  
F96

**«GYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың  
XX Халықаралық ғылыми конференциясы = XX Международная  
научная конференция студентов и молодых ученых «GYLYM JÁNE  
BILIM – 2025» = The XX International Scientific Conference for  
students and young scholars «GYLYM 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

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

## СЕКЦИЯ 2

### СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDSAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

## Подсекция 2.2

### Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған ai дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IoT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

### Подсекция 2.3

#### Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
<b>Подсекция 2.4</b>		
<b>Информационная безопасность</b>		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Рамагуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

### СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

## CRYSTALS-KYBER АЛГОРИТМІН РЕСУРСЫ ШЕКТЕУЛІ ҚҰРЫЛҒЫЛАРҒА ОҢТАЙЛАНДЫРУ

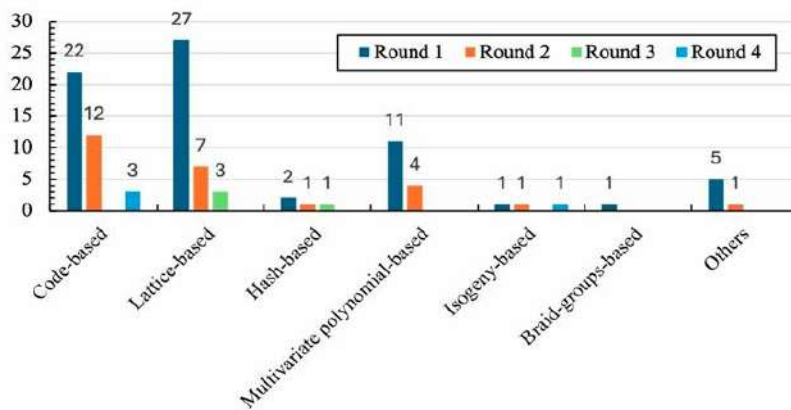
Жарасхан Назира Жарасханқызы, Қайуов Еркебұлан Керімұлы  
[8934263@gmail.com](mailto:8934263@gmail.com), [Yerik.kai@gmail.com](mailto:Yerik.kai@gmail.com)

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті  
Ақпараттық қауіпсіздік кафедрасының докторанттары, Астана, Қазақстан  
Ғылыми жетекшісі– ф.м.-ғ.к, Оспанова Адеми Бекжановна

Криптографияның даму тарихында посткванттық криптографияға көшумен байланысты түбегейлі жаңа кезеңнің қалыптасып келе жатқаны байқалады. 1990-шы жылдардың басынан бастап кванттық алгоритмдердің теориялық негіздері қалыптастырылып, қазіргі заманғы криптографиялық жүйелерге тиімді шабуыл жасауға қабілеттілігі дәлелденді. Сонымен қатар, есептеу қуаты жеткілікті кванттық құрылғылар пайда болған жағдайда қолданыстағы криптографиялық протоколдардың басым көпшілігінің осалдығы туралы ғылыми негізделген дәлелдер ұсынылды. Ғылыми қауымдастық кванттық компьютерлердің жақын болашақта жасалып шығарылатынына еш күмән келтірмейді. Бұған қоса, кванттық технологиялардың қазіргі даму жылдамдығы, мұндай құрылғылардың алдын ала болжанғаннан әлдеқайда ертерек пайда болуы мүмкіндігін көрсетеді.

Шордың жұмыстары [1] және кейінгі зерттеулер кванттық алгоритмдердің классикалық машиналар үшін қиын болып есептелетін есептерді тиімді шеше алатынын көрсетті. Бұл қазіргі қолданыстағы криптожүйелердің сенімділігіне елеулі қауіп төндіреді. Кванттық есептеулер саласындағы заманауи жетістіктер бұл қауіптің ұлғаюына алып келді. Атап айтқанда, NIST сарапшыларының бағалауынша, қазіргі криптографиялық стандарттарды бұзуға қабілетті кванттық компьютердің 2030 жылға дейін пайда болу ықтималдығы 17–24% аралығында бағалануда [2]. Бұл жағдайда әсіресе ақпараттық қауіпсіздік протоколдарының негізінде жатқан алгоритмдер осал болып келеді. Сонымен қатар, кейбір болжамдарға сәйкес [3] кванттық тұрақты алгоритмдерге көшуге 10–15 жыл қажет болуы мүмкін. Алайда кванттық шабуыл қаупі бұдан әлдеқайда ерте туындауы ықтимал. Сондықтан посткванттық криптографияға шұғыл әрі үйлестірілген түрде көшу қажеттілігі туындап отыр.

АҚШ-тың Ұлттық стандарттар және технологиялар институты (NIST) 2016 жылы посткванттық криптографиялық алгоритмдерді іріктеу және стандарттау үдерісін бастады [4]. Бұл бастама аясында бірнеше перспективалы үміткерлер ұсынылды. Олардың ішінде торларға негізделген криптография (Lattice-based Cryptography), көпмүшелік криптография (Multivariate Cryptography) және кодтарға негізделген криптография (Code-based Cryptography) секілді бағыттар қамтылды. Іріктеу төрт раундтан тұратын кезең-кезеңімен жүргізілді. Бірінші раундта 60-тан астам өтінім қабылданып, соңғы раундтарда тек ең мықты үміткерлер ғана қалды. **1-суретте** [5] әрбір раундтан өткен криптографиялық алгоритмдердің түрлері бойынша үлестірілуі көрсетілген. Мұнда торлық және кодтық тәсілдердің айқын басымдығы байқалады.



**Сурет 1** – NIST стандартизациялау процесінің раундтары бойынша посткванттық алгоритмдер түрлерінің үлестірілуі [5]

2024 жылдың тамыз айында CRYSTALS-Kyber және CRYSTALS-Dilithium алгоритмдерінің финалдық стандарттарының жариялануы посткванттық криптография тарихындағы маңызды оқиға болды [6]. Аталған алгоритмдер қазіргі таңда жаһандық деңгейдегі қауіпсіздік протоколдарына, соның ішінде TLS және басқа да кілт алмасу мен цифрлық қолтаңба жүйелеріне енгізу үшін қарастырылуда. Айта кетерлігі, бұл стандарттар ресми түрде бекітілмей тұрып-ақ, алдыңғы қатарлы мамандар посткванттық алгоритмдерді тәжірибе жүзінде зерттеп, біріктіріп және сынақтан өткізе бастаған. Сонымен қатар, баламалы тәсілдер бойынша да зерттеулер жалғасуда. Солардың қатарында хэшке негізделген криптография (Hash-based Cryptography) сынды бағыттар посткванттық қорғау құралдарының арсеналын кеңейтуге үлес қосуда.

Кванттық есептеулерден туындайтын жоғары деңгейдегі қауіптерді және шектеулі ортада орнықты қауіпсіздік шешімдерін енгізу қажеттілігін ескере отырып, есептеу қуаты шектеулі құрылғыларға бейімделген мамандандырылған қауіпсіздік архитектураларын әзірлеуге ерекше көңіл бөлінуде. Посткванттық криптографиядағы жетекші алгоритмдердің бірі болып саналатын CRYSTALS-Kyber алгоритмін қолдану барысында процессорлық жүктемені және энергия тұтынуды азайту мақсатында өзгертулерді қажет етеді [7]. Бұл ретте қауіпсіздік параметрлерін нақты қолдану сценарийіне қарай икемдеп таңдау мүмкіндігі де маңызды болып табылады.

Көптеген посткванттық алгоритмдер жоғары есептеу күрделілігімен және елеулі ресурстық талаптарымен сипатталады. Бұл олардың есептеу ресурсы шектеулі құрылғыларда, соның ішінде IoT құрылғыларында, кірістірілген жүйелерде, жергілікті деңгейдегі желілік құрылғылар мен мобильді есептеу платформаларында қолданылуын шектейді. Мұндай құрылғыларда есептеу қуатының, энергия тұтынудың және архитектуралық мүмкіндіктердің шектеулілігі байқалады. Посткванттық алгоритмдерді осындай жағдайларда тиімді қолдану үшін жад көлемі, процессор қуаты және энергия тұтыну талаптарын ескере отырып, оларды оңтайландыру қажет. Бұл мақалада аталған мәселелер мен қолжетімді аппараттық ресурстарды бағалау мәселелері қарастырылады. Жүзеге асыру және тестілеу үшін әмбебап әрі қолжетімді есептеу модулі болып табылатын **Raspberry Pi** платформасын пайдалану ұсынылады. Бұл платформа зерттеу мен қолданбалы міндеттерді шешуге кеңінен бейімделген.

Сонымен қатар, гибриді криптографиялық жүйелерді, әсіресе посткванттық механизмдерді қолдануға негізделген бағыттарды ғылыми тұрғыда зерттеу келешегі зор болғанымен, әлі де жеткілікті дәрежеде зерттелмегенің атап өткен жөн [8]. Солардың ішінде ерекше назар аударуға тұрарлық бағыттардың бірі — CRYSTALS-Kyber алгоритмін ресурсы шектеулі құрылғыларда, мысалы, Raspberry Pi платформасында қолдануға бейімдеу болып

табылады. Бұл платформаны таңдау негізі үш фактормен түсіндіріледі: кең таралғандығы, архитектуралық өкілділігі және IoT-ортасына қолданылатындығы, бұл оны энергия тиімді шешімдерді сынау үшін оңтайлы етеді. Kyber алгоритмін оңтайландыру энергия тұтынуды азайтуға және өнімділікті арттыруға бағытталған. Бұл ретте криптографиялық тұрақтылық деңгейін сақтау — посткванттық қауіпсіздік стандарттарына көшу жағдайында ерекше маңызды талап болып табылады.

Ғылыми-зерттеу жұмысының практикалық қолданылуы ретінде посткванттық криптографияны Raspberry Pi миникомпьютерлері негізінде іске асыруға бағытталған, қорғалған әрі ақауға төзімді аппараттық-бағдарламалық жүйені әзірлеу ұсынылады. Мұндай жүйе мамандандырылған әрі аса маңызды ақпаратпен жұмыс істейтін құрылымдарда мәліметтерді жеткізу кезінде жоғары қауіпсіздік, сенімділік және істен шығуға тұрақтылық деңгейін қамтамасыз етуге қабілетті болуы тиіс. Зерттеу аясында ақпараттың құпиялығы, тұтастығы және қолжетімділігі тәрізді негізгі қауіпсіздік қағидаттарын, соның ішінде ақаулар, кибершабуылдар немесе тұрақсыз желілік инфрақұрылым жағдайында да сақтау қажеттігі туындайды. Бұл мақсатта екі Raspberry Pi құрылғысы негізінде қосарлау және автоматты түрде ауысу мүмкіндігі бар ақауға төзімді архитектураны іске асыру ұсынылады. Сонымен қатар, қысқа хабарламаларды сенімді қорғау үшін симметриялық және асимметриялық шифрлау әдістерін біріктіретін гибриді криптографиялық жүйені әзірлеп, жүйеге енгізу көзделеді.

Сондай-ақ практикалық іске асырудың маңызды бағыттарының бірі ретінде **CRYSTALS-Kyber** алгоритмін **Raspberry Pi** платформасында оңтайландыруды атап өтуге болады. Бұл ретте құрылғының аппараттық шектеулері мен ақпараттық қауіпсіздік талаптары ескерілуі тиіс. Осыған байланысты зерттеу мен әзірлеу үдерістерін келесі негізгі бағыттарға шоғырландыру ұсынылады:

1. Raspberry Pi платформасына бейімделген, кілттерінің өлшемі қысқартылған және есептеу жылдамдығы оңтайландырылған CRYSTALS-Kyber алгоритмінің іске асырылған нұсқасы.

2. Алгоритмді оңтайландыру кезінде қауіпсіздік тұрақтылығын растау, қауіпсіздіктің төмендеу тәуекелдерін егжей-тегжейлі талдау

3. CRYSTALS-Kyber алгоритмін ұлттық ақпараттық қауіпсіздік стандарттарымен интеграциялау бойынша ұсыныстар әзірлеу, сондай-ақ IoT құрылғыларына арналған қорғалған байланыс арналарының сенімділігін арттыруға бағытталған тәсілдерді негіздеу.

4. Raspberry Pi және бұлттық симуляторлар негізінде іске асырылған, шектеулі ресурстарға ие құрылғылар арасында деректерді беру үшін қорғалған байланыс арнасының модельдеу.

5. Шектеулі есептеу ресурстары және IoT жүйелері бар жүйелерде посткванттық алгоритмдерді практикалық қолдану тәсілдерін ұлттық қауіпсіздік ерекшеліктерін ескере отырып талдау.

CRYSTALS-Kyber алгоритмін Raspberry Pi платформасында іске асыру міндетін шешуге арналған тәсілдердің бірі - алгоритмді құрылғының шектеулі ресурстарын ескере отырып кешенді бейімдеу және оңтайландыру. Бұл тәсіл аясында келесі шаралар қарастырылады:

1. CRYSTALS-Kyber алгоритмін Raspberry Pi платформасына бейімдеп іске асыру. Raspberry Pi таңдалуы оның ықшам форм-факторымен, кеңейтуге арналған қосымша модульдерінің мол болуымен, сондай-ақ алынған нәтижелерді өзге жобаларға енгізу мүмкіндіктерімен түсіндіріледі.

2. Алгоритмді бейімдеу және оңтайландыру барысында кілттердің өлшемін қысқарту, есептеу әдістерін жылдамдату, дайын кітапханаларды пайдалану және есептеу процестерін параллельдеу сияқты модификациялар қарастырылады, бұл жүйенің жұмыс жылдамдығын арттырумен қатар энергия тиімділігін де жақсартады.

Сонымен қатар, қолданылатын операциялық жүйені, бағдарламалау құралдарын және шағын экрандарға бейімделген пайдаланушы интерфейсін дұрыс таңдаумен бірге жүйенің сенімділігіне, ақауға төзімділігіне және жауап беру жылдамдығына қойылатын талаптар да ескерілуі қажет.

3. Зерттеу және тестілеу. Қауіпсіздік деңгейінің қолайлы деңгейде сақталуын растау, сондай-ақ тәуекелдерді бағалау.

4. Ұлттық қауіпсіздік стандарттарымен интеграция.

4.1) Қолданылған әдістемелер мен алынған нәтижелердің Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құжаттарға қайшы келмеуін зерттеу.

4.2) Алынған нәтижелерді елдегі қолданыстағы немесе стандартталған криптографиялық тәсілдермен бірлесіп пайдалану бойынша идеяларды қалыптастыру.

5. Алынған нәтижелерді практикалық тұрғыда қолдану мүмкіндіктері (сипаттамалар, негіздемелер және үлгілік модельдер).

5.1) Арнайы міндет ретінде, мысалы, шектеулі ресурстарға ие бір құрылғыдан екіншісіне шифрланған деректерді беру үшін қорғалған арна құруды атауға болады.

5.2) Бұдан бөлек, келесі техникалық орталар зерттеледі:

а) Raspberry Pi құрылғылары,

б) виртуализациясы бар жергілікті машиналар (мысалы, dockers),

в) посткванттық алгоритмдерді тестілеуге арналған бұлттық модельдеу ортасы.

Бұл үш жағдайдың (а–в) әрқайсысы үшін IoT саласындағы жекелеген аспектілерді жүзеге асырудың ерекшеліктері талданып, үлгілік мысалдар келтіріледі.

Барлық үш жағдайда (а)-дан в)-ға дейін) IoT-тың кейбір аспектілерін жүзеге асыру ерекшеліктері қарастырылып, модельдік мысал келтіріледі.

Криптографиялық оңтайландырумен қатар, зерттеу барысында шағын көлемді құрылғыларға бейімделген пайдаланушы интерфейсін, операциялық жүйені және әзірлеу құралдарын таңдауды қоса алғанда, қолданылатын бағдарламалық-техникалық құралдар базасы да қарастырылады.

Осылайша, кванттық есептеулердің дамуы қазіргі заманғы криптографиялық протоколдар, әсіресе асимметриялық шифрлау жүйелері үшін елеулі қауіп төндіреді. Бұл өз кезегінде посткванттық алгоритмдерге көшу қажеттілігін туындатады. NIST стандартына енген CRYSTALS-Kyber алгоритмі жоғары криптографиялық тұрақтылықты, тиімділікті және масштабталу мүмкіндігін көрсетеді. Сонымен қатар, ол ресурсы шектеулі құрылғыларда, соның ішінде IoT жүйелерінде, кірістірілген жүйелерде және Raspberry Pi секілді микрокомпьютерлерде қолдануға ыңғайлы. CRYSTALS-Kyber алгоритмін бейімдеу және оңтайландыру оны гетерогенді ортада криптографиялық тұрақтылықты жоғалтпай қолдануға мүмкіндік береді. Гибридті криптографиялық схемаларды әзірлеу және оларды әрі қарай стандарттау ұлттық талаптарды ескеретін жаңа протоколдарға қауіпсіз көшуге мүмкіндік береді. Бұл осы бағыттағы зерттеулердің өзектілігін және практикалық маңыздылығын айқындайды.

### Қолданылған әдебиеттер тізімі

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124-134.

2. Chen L., Moody D., Liu Y.K. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8413. 2022. P. 12. (URL: <https://doi.org/10.6028/NIST.IR.8413>)

3. National Institute of Standards and Technology. PQC Benchmarking Report. 2022.

4. National Institute of Standards and Technology (NIST). Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. December 2016. 23 p. (URL: <https://csrc.nist.gov/Projects/post-quantum-cryptography>)

5. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* 2024, 12, 241. <https://doi.org/10.3390/technologies12120241>

6. Barton M., et al. Benchmarking Post-Quantum Cryptography on ARM Cortex-M // *Cryptographic Hardware and Embedded Systems - CHES 2021*. 2021. P. 319-338.

7. Cherkaoui Dekkaki S., El Idrissi N., Ez-Zahraouy H. Comparative analysis of post-quantum cryptographic algorithms for IoT security // *Journal of Information Security and Applications*. 2024. Vol. 78. P. 103678. (DOI: 10.1016/j.jisa.2024.103678)

8. Bindel N., Schanck J.M., Schuldt J.C.N., Veitch D. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange // *Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science*, vol 11505. Springer, Cham. 2019. P. 206-226.

УДК 004.056.5

## **ЗАМАНАУИ ОПЕРАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕГІ ЖАДЫ ДАМПЫ КЕСКІНІН АЛУ ҚҰРАЛДАРЫН ТАЛДАУ ЖӘНЕ САЛЫСТЫРУ**

**Жолдасбаев Мағжан Әбілтайұлы**

[magzhanzholdasbaev@mail.ru](mailto:magzhanzholdasbaev@mail.ru)

Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс  
магистранты, Астана, Қазақстан  
Ғылыми жетекшісі – Ж.Сауханова

Қазіргі ақпараттық жүйелер жоғары архитектуралық күрделілікпен және өңделген деректердің айтарлықтай көлемімен сипатталады. Мұндай жағдайларда жедел жад күйін талдау келесі мәселер үшін өте маңызды болып табылады:

1) Критикалық ақауларды диагностикалау және ақаулықтарды жою (BSOD, kernel panic)

2) Ақпараттық қауіпсіздік инциденттерін зерттеу

3) Цифрлық деректерді криминалистикалық талдау

Дәстүрлі тіркеу әдістері жүйенің ақаулық кезіндегі жағдайын толық түсіну үшін жиі жеткіліксіз және бұл жады дампын қажет ақпарат көзі етеді.

Жады дампы әдетте жүйе қатесі немесе бағдарлама ақауы орын алған кезде автоматты түрде жасалады. Бұл дампы пайдалану арқылы жүйенің немесе бағдарламаның қай жерінде ақау болғанын анықтауға болады.

Жады дампын бірнеше негізгі критерийлер бойынша жіктеуге болады, оның ішінде егжей-тегжейлі зерттеу деңгейі, қол жеткізу мақсаты, кескінін алу әдісі және сақтау пішімі бойынша қарастырылады. Төменде егжей-тегжейлі жүйелеу көрсетілген.

1. Жады дампын мәліметтерді толық қамту деңгейі бойынша жүйелеу

1.1. Толық жад дампы жүйенің жадындағы барлық деректердің көшірмесі, ол жүйенің жұмыс істеп тұрған бағдарламалары мен компоненттерінің жағдайын сақтайды. Дампта процессорлардың регистрлері, бағдарламалардың және драйверлердің ішкі күйі туралы ақпараттар болады. Бұл дампы ақауларды терең зерттеуге мүмкіндік береді, себебі барлық жүйелік деректер қамтылады. Дегенмен, оның көлемі үлкен болуы мүмкін, бұл оны сақтау мен өңдеуді қиындатады. Толық жад дампы күрделі қателіктер мен құлдырауларды анықтауға