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 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

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 аі 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

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

УДК 004.056.55:004.383.1

CRYSTALS-KYBER АЛГОРИТМІН РЕСУРСЫ ШЕКТЕУЛІ ҚҰРЫЛҒЫЛАРҒА ОҢТАЙЛАНДЫРУ

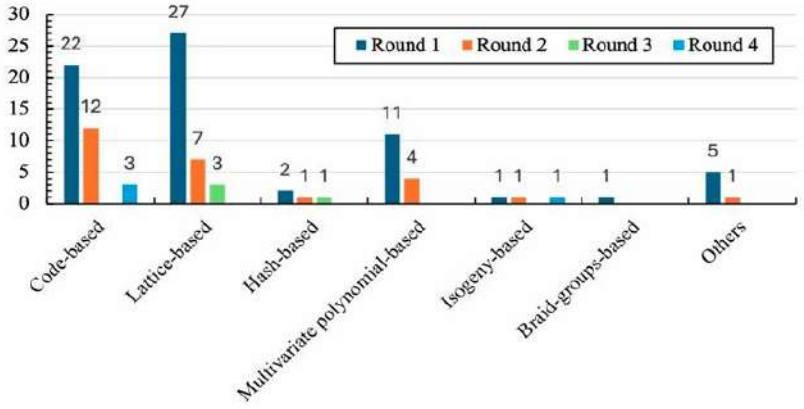
Жарасхан Назира Жарасханқызы, Қайупов Еркебұлан Керімұлы
8934263@gmail.com, Yerik.kai@gmail.com

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 постквanттық 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 постквanттық криптографияға шұғыл әрі үйлестірілген түрде көшу қажеттілігі туындап отыр.

АҚШ-тың Ұлттық стандарттар және технологиялар институты (NIST) 2016 жылы постквanттық 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 постквантық алгоритмдер түрлерінің үлестірілуі [5]

2024 жылдың тамыз айында CRYSTALS-Kyber және CRYSTALS-Dilithium алгоритмдерінің финалдық стандарттарының жариялануы постквантық 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 постквантық 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 постквантық 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. Постквантық 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 постквантық 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. Постквантық 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, гибридті криптографиялық жүйелерді, әсіресе постквантық 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 — постквантты қауіпсіздік стандарттарына көшу жағдайында ерекше маңызды талап болып табылады.

Ғылыми-зерттеу жұмысының практикалық қолданылуы ретінде постквантты 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 құпиялылығы, 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 гибридті 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 постквантты 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),л

в) постквантық 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 постквантық 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
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 дампты 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 дамп 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