

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. «EDCAFE 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 «ИОТ 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
Подсекция 2.4		
Информационная безопасность		
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. «Neuvector 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. Раматуллаев 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

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 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

көмектеседі. Ол жүйенің ішкі жұмысын талдауға, сондай-ақ жүйені оңтайландыру және тұрақтылығын қамтамасыз ету үшін маңызды. Бұл құрал бағдарламалау, жүйелік диагностика, ақпараттық қауіпсіздік және серверлік жүйелерде де қолданылады. Толық жады дампын алуға арналған құралдар ретінде мыналарды қарастыруға болады:

- a) Windows: WinDbg (.dump /ma), Belkasoft RAM Capturer;
- b) Linux: dd + /dev/mem, LiME;
- c) macOS: osxpmem;

1.2. Ядро дампы жүйенің ядросының жұмысын сипаттайтын жадтың көшірмесі, ол жүйе құлаған кезде автоматты түрде жасалады. Бұл дампы тек жүйелік деңгейдегі деректерді, атап айтқанда, ядроның күйі мен драйверлердің жұмысын қамтиды. Талдау арқылы жүйе әкімшілері немесе бағдарламашылар ядроның ақауын анықтап, оны түзету жолдарын іздей алады. Ядро дампы жүйенің тұрақтылығын қамтамасыз ету және жүйелік ақауларды жөндеу үшін қолданылады. Сонымен қатар, ол жүйенің қауіпсіздігін жақсарту мақсатында жүйелік ақауларды зерттеуге арналған құрал болып табылады. Дампта ядроның күйі, жүйелік деректер, драйверлер мен модульдер, сондай-ақ қате туралы ақпарат қамтылады. Кейде ядро дампы пайдаланушы кеңістігіндегі маңызды деректерді де сақтап, жүйенің құлдырауы немесе қатесі туралы қосымша ақпарат береді. Толық дамппен салыстырғанда артықшылығы өлшемі анағұрлым аз әрі драйверлермен критикалық қателелерді диагностикалауға жеткілікті.

Аталған дампының кескіні алу құралдарына мысал ретінде:

- a) Windows: Control Panel → System → Advanced → Startup and Recovery баптауын;
- b) Linux: kdump + crash утилитасын қарастыруға болады.

1.3. Минидампы (Small Memory Dump)

Минималды жад дампы (минидампы) жүйенің жұмыс істеп тұрған кезінде тек ең маңызды ақпаратты қамтитын шағын жад көшірмесі болып табылады. Бұл дампы жүйенің негізгі күйін, процесс идентификаторын және қатенің орын алған жерін ғана көрсетеді, сондықтан ол толық жад дампына қарағанда әлдеқайда аз орын алады. Минималды жад дампы жүйелік немесе бағдарламалық қателерді жылдам анықтауға мүмкіндік береді, бірақ толық терең талдауды қамтамасыз етпейді. Минималды жад дампының негізгі артықшылығы жылдам талданады және ресурстарды үнемдейді. Бұл дампы жүйе деңгейіндегі ақауларды тез анықтау үшін пайдалы, себебі ол тек маңызды ақпаратты сақтайды. Сонымен қатар, минималды жад дампының қолданылуы қарапайым әрі жиі кездесетін жүйелік қателерді зерттеуге ыңғайлы.

Минидампы кескінін алушы құралдарға:

- a) Windows: Minidump (WER жүйесінде конфигурацияланады)
- b) Linux: systemd-coredump

1.4. Пайдаланушы процесінің дампы (User-mode Process Dump)

Пайдаланушы процесінің дампы жүйе қатесі немесе құлдырауы кезінде пайдаланушы кеңістігіндегі процестің жадын сақтайтын файл. Дампта процестің стек деректері, жадының мазмұны, регистрлер мен айнымалылар сияқты маңызды ақпараттар сақталады. Бұл дампы пайдалану арқылы бағдарламашылар процестің қателіктерін анықтап, түзету жолдарын таба алады. Оның көлемі бірнеше мегабайттан аспайды, бұл оны өңдеуді жеңілдетеді. Дампта процесс идентификаторы (PID) мен қате туралы ақпарат, сондай-ақ сигналдар мен кідірістер туралы мәліметтер де болуы мүмкін. Дампы қолға түсіруге арналған құралдарға мыналар жатады:

- a) Windows: ProcDump, Task Manager;
- b) Linux: gcore, gdb;
- c) macOS: lldb + process save-core;

2. Жады дампын алу мақсаты бойынша жүйелеу

Бұл кесте жадтың дампын алу мақсатында қолданылатын құралдар мен операциялық жүйелерді көрсетеді, ал әрбір мақсаты бойынша сәйкес критерийлер анықталған.

Құрал түрі	Мақсаты	Құралдар	Операциялық жүйе
Түзету	Бағдарламалық жасақтамадағы қателерді іздеу, жадтың ағып кетуін талдау	WinDbg, gdb, lldb	Windows, Linux, macOS
Криминалистикалық	Зиянды бағдарламалардың іздерін іздеу, артефактілерді алу	Volatility, LiME, Rekall	Windows, Linux
Өнімділік	Қолданбаның өнімділігін оңтайландыру, жадты пайдалануды талдау	ProcDump, perf (Linux), Instruments (macOS)	Windows, Linux, macOS
Жүйелік	BSOD/kernel panic диагностикасы, драйверді талдау	kdump, WinDbg, crash	Linux, Windows

Кесте 1. Жады дампының кескіні алу құралдарының мақсаты бойынша жіктелуі.

3. Құралдар көмегімен жады дампын қолға түсіру процессі
 - 3.1. Ядро дампын алу LiME (Linux Memory Extractor) құралы

```
[root@mag ~]# insmod lime-2.6.32-431.5.1.el6.x86_64.ko "path=/root/mem.img format=lime"
[root@mag ~]# ls -lah /root/mem.img
-r--r--r--. 1 root root 1.0G Mar 9 08:11 /root/mem.img
```

Сурет 1. Ядро дампын алу барысы.

LiME (Linux Memory Extractor) Linux жүйесінде жадты толық бейнелеу жасауға мүмкіндік беретін ашық кодты құрал. Ол жадтың барлық мәліметтерін шығаруға және сақтауға арналған, әсіресе қауіпсіздік инциденттері мен қылмыстық тергеулерде пайдалы. LiME жадтағы процестердің, жүйелік ақпараттардың және бағдарламалық деректердің толық көшірмесін сақтай алады. Бұл құрал цифрлық криминалистикада жүйенің күйін зерттеу үшін қолданылады, сонымен қатар зиянды бағдарламаларды анықтауға көмектеседі. LiME жадты RAW және EWF форматтарында сақтай алады, бұл зерттеулер үшін ыңғайлы болып табылады. Ол Linux жүйесінің түрлі архитектураларын қолдайды, соның ішінде ARM және x86. LiME жүйені зерттеу кезінде нақты ақпаратты алу үшін қажетті құрал болып табылады.

- 3.2. Процесс дампын алу gcore құралы

```

maga@maga:~/Desktop$ ls
maga@maga:~/Desktop$ sudo gcore 9855
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
0x00007f222be2780c in pselect () from /lib/x86_64-linux-gnu/libc.so.6
warning: Memory read failed for corefile section, 4096 bytes at 0xfffffffff60000.
Saved corefile core.9855
[Inferior 1 (process 9855) detached]
maga@maga:~/Desktop$ ls
core.9855
maga@maga:~/Desktop$ █

```

Сурет 2. Процесс дампын қолға түсіру барысы.

gcore Linux жүйесінде жұмыс істеп тұрған процестің жадын жедел түрде түсіріп алуға мүмкіндік беретін құрал. Ол белгілі бір процестің жадын толық немесе ішінара көшіру арқылы, оның күйін сақтап, кейіннен талдауға мүмкіндік береді. gcore процесстің жадын core dump файлы ретінде сақтайды, бұл деректер қателіктерді немесе өнімділік мәселелерін зерттеуге пайдалы болады. Бұл құрал әсіресе бағдарламалық қателерді, құлауларды немесе өнімділік ақауларын анықтау кезінде қолданылады. Ол жұмыс істеп тұрған процестердің күйін терең зерттеуге мүмкіндік береді, бұл тергеу немесе талдау үшін маңызды болуы мүмкін. gcore процесстің барлық жадын, оның ішінде ішкі деректер мен айнымалыларды сақтайды, бұл бағдарламаның нақты күйін көрсетуге көмектеседі. Бұл құрал жүйенің ақауларын немесе қосымшаның қатесін табу үшін тиімді қолданылады. Сонымен қатар, gcore басқа процестерге әсер етпей, тек бір процестің жадын түсіруге мүмкіндік береді. Алынған мәліметтер кейінірек аналитикалық құралдармен талданып, қателіктер мен өнімділік мәселелері анықталады. gcore жалпы түрде жүйелік мониторинг пен қателіктерді түзету үшін кеңінен қолданылатын құралы болып табылады..

3.3. Процестің минидампын және жүйенің толық дампын алу ProcDump құралы

```

C:\Users\m_la\Documents\Procdump>procdump 6468

ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[09:40:15] Dump 1 initiated: C:\Users\m_la\Documents\Procdump\explorer.exe_210624_094015.dmp
[09:40:16] Dump 1 complete: 8 MB written in 0.5 seconds
[09:40:16] Dump count reached.

```

Сурет 3. Белгілі бір процесстің минидампын қолға түсіру барысы.

ProcDump Windows жүйесінде процестердің жадын түсіру және оларды талдау үшін қолданылатын құрал. Ол процестердің жадын core dump түрінде сақтап, жүйелік ақауларды, бағдарлама қателіктерін немесе өнімділік мәселелерін анықтауға көмектеседі. ProcDump құралын әсіресе жүйе қателіктері немесе апаттық жағдайларды тергеу кезінде қолдануға болады. Бұл құрал нақты уақытта жұмыс істеп тұрған процестердің жадын түсіріп, кейіннен талдауға мүмкіндік береді. ProcDump егер процесс белгіленген шарттарға сәйкес тоқтап немесе қателессе, жадты автоматты түрде түсіре алады. Ол сондай-ақ, процесс тұрақты түрде жауап бермеген кезде немесе басқа белгілі бір шарттар орындалғанда dump файлдарын жасауға арналған. ProcDump алынған жад файлдарын түрлі дебаггерлермен немесе талдау құралдарымен тексеруге мүмкіндік береді. Оның қолданылуы жүйелік қауіпсіздікті

қамтамасыз ету және бағдарламалық ақауларды түзету мақсатында кеңінен таралған. ProcDump — ақауларды анықтау және жүйелік қателіктерді түсіну үшін аса маңызды құрал болып табылады.

```
C:\Users\m_la\Documents\Procdump>procdump -ma -i C:\dumps

ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Set to:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
  (REG_SZ) Auto = 1
  (REG_SZ) Debugger = "C:\Users\m_la\Documents\Procdump\procdump.exe" -accepteula -ma -j "C:\dumps" %ld %ld %p

Set to:
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\AeDebug
  (REG_SZ) Auto = 1
  (REG_SZ) Debugger = "C:\Users\m_la\Documents\Procdump\procdump.exe" -accepteula -ma -j "C:\dumps" %ld %ld %p

ProcDump is now set as the Just-in-time (AeDebug) debugger.
```

Сурет 4. Жүйенің толық дампын алу.

ProcDump құралын қолдана отырып, толық жадтың дампын алу үшін алдымен процесс идентификаторын (PID) анықтау қажет. Бұл үшін Task Manager немесе командалық жол арқылы процесті табуға болады. Процесстің толық жадын алу үшін -ma параметрін пайдалану керек, ол процесс туралы барлық ақпаратты, соның ішінде барлық айнымалылар мен буферлерді сақтайды. Бұл үшін 4-суретке назар аударсақ болады. Бұл команда процесстің барлық жадын, оның ішінде ядро деңгейіндегі ақпаратты да қамти отырып, көрсетілген файлға сақтайды. Алынған дампы файлы кейінірек қателіктерді немесе өнімділік мәселелерін тергеу үшін талданады. ProcDump жадтың толық көшірмесін алу кезінде жүйені ешқандай қиындыққа ұшыратпайды, себебі ол тек бір процесті ғана зерттейді. Осылайша, құралдың көмегімен жадыдағы маңызды деректерді сақтап, олардың күйін кейінірек толық зерттеуге болады.

4. Дампы түрлерін алуды салыстыру

Дампы түрлерін салыстыру кестесін деректер көлемі, жасалу уақыты, талдау мүмкіндігі және қолдану мысалы критерийлері бойынша жүйелеуге болады.

Критерий	Толық дампы	Ядро дампы	Минидампы	Процесс дампы
Деректер көлемі	100% RAM	30–50% RAM	<2 МБ	Процеске байланысты
Жасалу уақыты	Ұзақ	Орташа	Қас-қағым	Жылдам
Талдау	Максималды толық	Драйверлер/ядро	Негізгі	Белгілі процесс
Қолдану мысалы	Криминалистика	BSOD талдауы	Жылдам диагностика	Бағдарлама отладкасы

Кесте 2. Дампы түрлерінің салыстыру кестесі

Қорытынды

Жады дампытарын кескінін алу құралдары жүйелердің тұрақтылығы мен қауіпсіздігін қамтамасыз ету үшін өте маңызды рөл атқарады. Бұл құралдар бағдарламалық қателіктерді, жүйелік ақауларды, өнімділік мәселелерін анықтауға және тергеуге мүмкіндік береді. Толық дампытар, мысалы, WinDbg және LiME, күрделі жүйелік ақауларды терең зерттеу үшін

алмастырылмайды, себебі олар жүйенің барлық ақпаратын қамтып, қателіктер мен ақауларды егжей-тегжейлі талдауға мүмкіндік береді. Ядро дампы, мысалы, kdump және WinDbg, драйверлер мен BSOD (Blue Screen of Death) диагностикасы үшін өте тиімді, себебі олар тек жүйенің ядросындағы қателіктерді анықтауға бағытталған. Қосымшаларды жылдам отладкалау және ақауларды тез анықтау үшін ProcDump және gcore сияқты процесс дампы қолданылады, өйткені олар тек белгілі бір процестердің күйін талдауға мүмкіндік береді. Минидампы, мысалы, Windows WER және systemd-coredump, бастапқы талдау жасауға арналған, себебі олар толық дампыға қарағанда аз көлемде ақпарат сақтайды, бірақ жүйедегі маңызды қателіктерді анықтауға болады. macOS жүйесінде osxrmem және lldb сияқты құралдар жадының толық және егжей-тегжейлі талдауын қамтамасыз етеді. Ал Volatility криминалистика саласында әмбебап құрал ретінде кеңінен қолданылып, әртүрлі платформаларда жады талдауға мүмкіндік береді. Жады дампын жасау құралының таңдауы нақты міндетке байланысты: жүйелік ақауларды тергеу үшін WinDbg және crash жақсы таңдау болса, процестердің жұмысын талдау үшін ProcDump және gcore қолданылады. Linux және macOS жүйелерінде толық талдау үшін LiME және osxrmem сияқты құралдар пайдаланылса, Windows жүйесінде дампын жасау үшін WinDbg және басқа да арнайы құралдар қолданылады. Құралдарды дұрыс таңдау жүйедегі қателіктерді анықтап, жоюға, сонымен қатар жүйелік қауіпсіздікті сақтауға көмектеседі. Бұл құралдардың барлығы тергеу, отладка және қауіпсіздік саласындағы маңызды аспектілерді қамтамасыз етеді, оларсыз күрделі мәселелерді шешу мүмкін болмас еді.

Қолданылған әдебиеттер тізімі

1. Русинович М., Соломон Д., Ионеску А. Windows Internals, Part 1. - 7th ed. - Microsoft Press, 2021. - 832 с.
2. Ligh M., Case A., Levy J. The Art of Memory Forensics. - Wiley, 2014. - 912 с.
3. Карпенко А.Б., Шакин В.Н. Анализ дампов памяти в цифровой криминалистике. - М.: ДМК Пресс, 2021. - 342 с.
4. Скляров Д.В. Современные методы анализа оперативной памяти. - СПб.: БХВ-Петербург, 2022. - 415 с.

ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫҢ ҚАУІПСІЗДІГІ ЖӘНЕ ОНЫҢ ҚОЛДАНЫЛУЫ

Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А.

¹Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.

Nurjigitkhovdabai@gmail.com, alih.marat.05@gmail.com

Ғылыми жетекші – Қазиева Н.М.

Аннотация

Бұл мақалада екі факторлы аутентификацияның (2FA) қауіпсіздігі қарастырылады және оның басқа аутентификация әдістерімен салыстырмалы талдауы жүргізіледі. Қазіргі таңда ақпараттық қауіпсіздіктің маңыздылығы арта түсуде, сондықтан пайдаланушылардың деректерін қорғау әдістері үздіксіз дамып келеді. 2FA – пайдаланушының жеке басын қосымша растау әдісі арқылы аутентификациялау технологиясы. Мақалада 2FA-ның тиімділігі, оның артықшылықтары мен кемшіліктері қарастырылады.

Кілттік сөздер: екі факторлы аутентификация (2FA), ақпараттық қауіпсіздік, киберқауіпсіздік, SMS-код, парольдік қауіпсіздік.