

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

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

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

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

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

**2025  
Астана**

УДК 001(06)  
ББК 72я631  
F96

**«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 «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. 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

Разработанная система позволяет эффективно анализировать тексты и веб-страницы на предмет достоверности информации, используя комбинацию машинного обучения и внешнего API. Гибкость в выборе метода проверки делает её устойчивой к возможным сбоям в работе API, а кеширование уже обработанных запросов значительно ускоряет работу и снижает нагрузку на систему.

Благодаря поддержке нескольких языков пользователи могут проверять информацию независимо от её исходного языка, что делает систему удобной и универсальной. Возможность анализа как текстов, так и веб-страниц повышает её функциональность, позволяя быстро оценивать достоверность новостных статей, блогов и других онлайн-ресурсов.

Таким образом, представленное решение является эффективным инструментом для борьбы с дезинформацией, предоставляя пользователям удобный и надежный способ проверки информации в условиях стремительного распространения фейковых новостей.

#### **Список использованных источников**

1. Nagarajan S., Sudha S.P. Evaluating Fake News Detection Models. October 2023.
2. Zhang B., Dai C., Deng Z. Fake News Detection and Analysis. October 2023.
3. Poorva S. Neural Fake Debt Net - Detection and Classification of AI Generated Fake News. May 2023.
4. Trivedi S., Jain M.K. Fake News Detection: A Study // Proceedings of the International Conference on Intelligent Computing, Communication and Information Security. Manipal University Jaipur. July 2023. P. 395-408.
5. Yuan L., Shen H., Shi L., Cheng N. An Explainable Fake News Analysis Method with Stance Information. August 2023.
6. Graves M., Li Y. Machine Learning Approaches for Fake News Detection: A Comprehensive Review // Journal of Information Science. 2023. Vol. 49, №6. P. 768-792.
7. Wang J., Liu L. Deep Learning Techniques in Fake News Detection: A Comparative Analysis // Information Processing & Management. 2023. Vol. 59, №5. P. 102637.
8. Chen Q., Zhang Y. Towards Explainable Fake News Detection: A Survey // ACM Computing Surveys. 2023. Vol. 56, №2. P. 1-34.
9. Jha S., Patel R. Fake News on Social Media: A Multimodal Approach to Detection // IEEE Transactions on Multimedia. 2023. Vol. 25, №11. P. 3153-3165.
10. Liu C., Wang F. Fake News Detection Using Natural Language Processing and Graph Embedding // Expert Systems with Applications. 2023. Vol. 191. P. 115567.

УДК 004.056

### **АНОМАЛИЯЛАРДЫ АНЫҚТАУ ӘДІСТЕРІН ТАЛДАУ**

**Ауесхан Назерке**

nazerkeaes@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Информатика  
кафедрасының магистранты, Астана, Қазақстан  
Ғылыми жетекші - Сагиндыков Каким Молдабекович

**Аннотация:** Бұл мақалада аномалияларды анықтау әдістерін талдау нәтижелері ұсынылған. Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, K-Means және DBSCAN әдістері қарастырылып, олардың деректер қауіпсіздігі мәселелеріне қолдану тиімділігі

зерттелді. Талдау нәтижесінде Isolation Forest және LOF әдістерінің деректердің өзара әрекеттесу моделін құрудағы нәтижелілігі анықталды.

**Түйінді сөздер:** Аномалияларды анықтау, ақпараттық қауіпсіздік, Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, K-Means, DBSCAN, деректер талдауы.

### **Кіріспе**

Аномалияларды анықтау — деректер жиынында қалыпты заңдылықтарға сәйкес келмейтін ерекше нүктелерді анықтау процесі. Бұл процесс деректер қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады.

1. Isolation Forest — бұл әдіс ағаш құрылымын қолданып, аномалияларды анықтайды. Әдіс мәліметтердің "оқшаулау" қасиеттерін пайдаланып, шеткері нүктелерді тез анықтайды.[1]

2. Local Outlier Factor (LOF) — әдіс деректер нүктелерінің локалды тығыздығын талдау арқылы аномалияларды анықтайды. LOF қалыпты нүктелер мен аномалиялардың арасындағы тығыздық айырмашылығын есепке алады.[2]

3. One-Class SVM — қолайлы гипержазықтық құру арқылы мәліметтердің қалыпты аймағын сипаттайды. Бұл әдіс әсіресе сызықтық емес деректерде тиімді қолданылады.[3]

4. K-Means — кластерлеу әдісі ретінде белгілі, бірақ оның көмегімен кластерлерден тыс нүктелерді аномалия ретінде белгілеуге болады.[4]

5. DBSCAN — тығыздыққа негізделген кластерлеу әдісі. Бұл әдіс тығыздықтары төмен аймақтарды аномалия ретінде қарастырады.[5]

Бұл зерттеуде аталған әдістердің артықшылықтары мен кемшіліктері салыстырмалы түрде талданып, олардың деректер қауіпсіздігін қамтамасыз етудегі қолдану мүмкіндіктері бағаланды.

#### **Зерттеудің мақсаттары:**

- Аномалияларды анықтау әдістерін талдау
- Ақпараттық қауіпсіздік модельдерін құруда ең қолайлы әдістерді анықтау.

#### **Талдау әдістемесі және негізгі талаптар**

Аномалияларды анықтау әдістерін бағалау үшін келесі негізгі критерийлер таңдалды:

1. Дәлдік: Әдістің аномалияларды дұрыс анықтау қабілеті. Бұл көрсеткіш жалпы мәліметтер жиынында аномалия ретінде дұрыс белгіленген нүктелердің пайызын білдіреді. Жоғары дәлдік — әдістің сенімділігінің негізгі белгісі.

2. Өнімділік: Мәліметтердің үлкен көлемімен жұмыс істегендегі жылдамдық пен есептеу тиімділігі. Бұл критерий әсіресе ауқымды мәліметтер жиынтығымен жұмыс істейтін жүйелер үшін маңызды.[6]

3. Тұрақтылық: Әдістің әртүрлі типтегі мәліметтерге тұрақтылығы мен олардың өзгешеліктеріне бейімделу қабілеті. Робастылық жоғары әдістер әртүрлі сценарийлерде жақсы жұмыс істейді.

4. Интерпретациялану : Әдістің нәтижелерін түсіндіру және оларды қолдану оңайлығы. Әсіресе қауіпсіздік мамандары үшін алгоритм нәтижелерін түсіну мен оларға сүйеніп шешім қабылдау маңызды.

5. Масштабталу: Әдістің үлкен деректер жиынтығымен жұмыс істеу мүмкіндігі. Масштабталу жоғары әдістер мәліметтердің ұлғаюына бейімделіп, тиімділігін сақтайды.

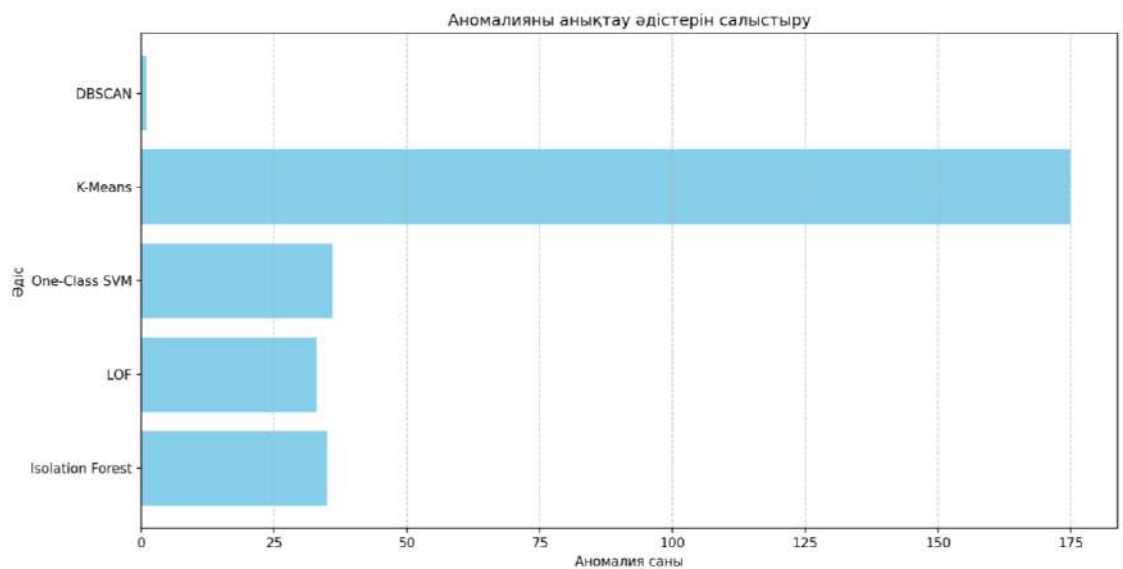
Әр әдіс 1-ден 5-ке дейінгі шкала бойынша бағаланады, мұнда 1 — ең төменгі көрсеткіш, ал 5 — ең жоғары көрсеткіш.

Әдіс	Isolation Forest	LOF	One-Class SVM	K-Means	DBSCAN
Дәлдік	5	5	4	3	4
Өнімділік	4	3	2	4	3
Тұрақтылық	5	4	3	3	4
Интерпретациялану	4	4	3	3	2
Масштабталу	5	4	3	4	3
Жалпы балл	23	20	15	17	16

Кесте 1. Әдістердің салыстырмалы бағалау

Жоғарыдағы кестеге(кесте 1) сәйкес, аномалияларды анықтауда ең тиімді әдіс Isolation Forest болып табылады. Бұл әдіс жоғары дәлдік, тұрақтылық және масштабталу көрсеткіштерімен ерекшеленеді, жалпы баллы 23. LOF әдісі де тиімді болып шықты, бірақ оның өнімділігі мен масштабталуы аздау, жалпы баллы 20. K-Means әдісі аномалияларды анықтауда сезімталдық танытып, жалған позитивтерге әкелуі мүмкін, жалпы баллы 17. DBSCAN мен One-Class SVM әдістері төменірек балл алды, себебі олар өнімділік пен интерпретациялану жағынан шектеулі болды.

Бағалау нәтижелері бойынша, Isolation Forest пен Local Outlier Factor (LOF) әдістері жоғары ұпай жинады, әсіресе олардың дәлдігі мен тұрақтылығы жағынан. Бұл әдістер аномалияларды анықтауда ең тиімді және деректер қауіпсіздігі үшін қолайлы болып табылады.



Сурет 1. Аномалияны анықтау әдістерін салыстыру

Сурет 1 жүргізген зерттеулерімнің нәтижесінде әзірленді. Логтар жинақталып, әртүрлі әдістер бойынша код жазылып, олардың қанша аномалияны анықтай алатыны талданды. Алынған мәліметтерді визуалды түрде көрсету арқылы әр әдістің артықшылықтары мен кемшіліктері анықталды.

Жоғарыда көрсетілген нәтиже бойынша, Isolation Forest және LOF әдістері ең тиімді аномалияларды анықтау құралдары ретінде ерекшеленді. Олар шынайы аномалияларды дәл және тұрақты түрде анықтай алады. Ал K-Means әдісі жалған позитивтердің көптігі салдарынан аномалияларды анықтауда шамадан тыс сезімталдық танытқан болуы мүмкін. Бұл нәтижелер талданған логтар негізінде ақпараттық қауіпсіздік жүйелерінде осы әдістерді қолдану үшін маңызды нұсқаулықтар береді.

### Қорытынды

Бұл зерттеу аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерін құру үшін қолдану мүмкіндіктерін талдауға бағытталған. Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, K-Means және DBSCAN әдістерінің тиімділігі салыстырылды. Нәтижелер бойынша, ең тиімді аномалияларды анықтау құралдары ретінде Isolation Forest және LOF әдістері таңдалды. Бұл әдістер шынайы аномалияларды дәл және тұрақты түрде анықтап, ақпараттық қауіпсіздік жүйелерінің сенімділігін арттырады.

Ал K-Means әдісі аномалияларды анықтауда шамадан тыс сезімталдық танытып, жалған позитивтердің көптігіне әкелуі мүмкін, бұл оның ақпараттық қауіпсіздік жүйелерінде қолданылуын шектейді. DBSCAN және One-Class SVM әдістері де кейбір жағдайларда тиімді болуы мүмкін, бірақ олардың тұрақтылығы мен өнімділігі ақпараттық қауіпсіздік талаптарына толық сәйкес келе бермейді.

Зерттеу нәтижелері аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерінде қолдану үшін маңызды нұсқаулықтар ұсынады. Isolation Forest және LOF әдістері жоғары дәлдік пен тұрақтылықпен аномалияларды анықтауға мүмкіндік береді, сондықтан олар ИБ жүйелерінде кеңінен қолдануға тиімді болып табылады. Болашақ зерттеулерде осы әдістерді жетілдіру мен әртүрлі жағдайларда сынақтан өткізу арқылы олардың тиімділігін одан әрі арттыруға болады.

### **Қолданылған әдебиеттер тізімі**

1. Xu H. et al. Deep isolation forest for anomaly detection //IEEE Transactions on Knowledge and Data Engineering. – 2023. – Т. 35. – №. 12. – С. 12591-12604.
2. Попова И. А. Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя Isolation Forest и Local Outlier Factor //StudNet. – 2020. – Т. 3. – №. 12. – С. 1460-1470.
3. Nuriddinovich K. S. Исследование обнаружения аномалий в сетевом трафике с использованием one-class svm //Journal of Modern Educational Achievements. – 2024. – Т. 1. – №. 1. – С. 214-222.
4. Ahmed M., Seraj R., Islam S. M. S. The k-means algorithm: A comprehensive survey and performance evaluation //Electronics. – 2020. – Т. 9. – №. 8. – С. 1295.
5. Deng D. DBSCAN clustering algorithm based on density //2020 7th international forum on electrical engineering and automation (IFEEA). – IEEE, 2020. – С. 949-953.
6. Котенко И. В. и др. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения //Информатика и автоматизация. – 2022. – Т. 21. – №. 6. – С. 1328-1358.

ӘӨЖ 004.056.5

### **КОРПОРАТИВТІК ЖЕЛІЛЕРДІ МОДЕЛЬДЕУ ЖӘНЕ ҚОРҒАУ**

**Бердибаев Көркем Сағындықұлы, Иманали Абылай Жандосұлы**

[b.korkem2004@gmail.com](mailto:b.korkem2004@gmail.com), [imanali\\_05@mail.ru](mailto:imanali_05@mail.ru)

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан  
Ғылыми жетекші – Казиева Назым Магидулловна

Бүгінгі цифрлық әлемде бизнес ақпараттық технологияларға толық тәуелді болғандықтан, корпоративтік желіні қорғау бірінші кезектегі маңызды міндетке айналады. Компаниялар күн сайын қарапайым вирустық шабуылдардан бастап, киберкылмыскерлердің