

**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

**«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, 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
<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

как OAuth или JWT для управления сессиями. Однако недавнее исследование, проведенное командой OpenAI, показало, что GitHub Copilot иногда может генерировать небезопасные фрагменты кода из-за ограничений в его обучающих данных, которые включают общедоступный код из репозитория GitHub, некоторые из которых могут содержать уязвимости. В отличие от этого, Cursor AI был разработан с акцентом на кибербезопасность, интегрируя инструменты безопасности и предоставляя рекомендации по кодированию, соответствующие принципам безопасного программирования. Ярким примером является его роль в оказании помощи разработчикам в создании безопасных RESTful API, рекомендуя такие меры безопасности, как проверка вводимых данных, шифрование и безопасная обработка токенов. Одним из примеров, когда Cursor AI оказался особенно полезен, была разработка нового мобильного банковского приложения, где разработчики столкнулись с трудностями при обеспечении безопасности транзакций и персональных данных. Благодаря рекомендациям Cursor AI они смогли внедрить надежные протоколы шифрования и предотвратить такие распространенные уязвимости, как внедрение SQL-инъекций. Кроме того, интеграция Cursor AI с такими инструментами безопасности, как Aikido, демонстрирует, как ИИ может проактивно обнаруживать уязвимости в режиме реального времени. Например, Aikido и Cursor AI использовались совместно для сканирования кодовой базы платформы электронной коммерции на предмет уязвимостей в системе безопасности. Сочетание подсказок по коду, основанных на искусственном интеллекте, и обнаружения угроз в режиме реального времени помогло выявить несколько критических уязвимостей, включая небезопасные методы хранения данных, которые затем были исправлены до того, как приложение было выпущено для широкой публики. Эти тематические исследования имеют решающее значение, поскольку они демонстрируют практическое применение инструментов искусственного интеллекта для повышения кибербезопасности, особенно в реальных сценариях, и подчеркивают уникальную направленность Cursor AI на обеспечение безопасности, как показано в таблице 1. В таблице сравниваются функции Cursor AI, ориентированные на безопасность, с другими инструментами искусственного интеллекта, что еще раз иллюстрирует его преимущества при разработке безопасного программного обеспечения.

#### **Список использованных источников**

1. Stallings, W. (2017). *Data and Computer Communications*. Pearson Education.
2. OpenAI. "AI-assisted coding: Enhancing software security and efficiency." *AI Research Journal*, 2023.
3. OWASP Foundation. "Secure coding practices: A guide for developers." *Cybersecurity Standards Report*, 2022.
4. Smith, J., & Lee, W. (2021). "Machine learning in cybersecurity: Applications and risks." *Cyber Defense Journal*.
5. Raza, S., Wallgren, L., & Voigt, T. (2013). "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad Hoc Networks*, 11(8), 2661-2674.

## **СТЕГАНОГРАФИЯ В КИБЕРБЕЗОПАСНОСТИ КАЗАХСТАНА**

**А.М. Султанов**

[salikoalpalmys@gmail.com](mailto:salikoalpalmys@gmail.com)

Бакалавр Евразийский национальный университет им. Л.Н. Гумилева, Астана  
Научный руководитель – Онгарбаева Айнагуль Игиликовна

*Аннотация*

*В данной статье рассматриваются современные аспекты применения стеганографии в сфере кибербезопасности Казахстана. Особое внимание уделено основным методам скрытия информации в цифровых объектах, таким как изображения, аудиофайлы, видеозаписи и сетевые протоколы. Проанализированы потенциальные преимущества стеганографии для защиты данных, а также угрозы, связанные с её использованием киберпреступниками. В статье рассматриваются существующие вызовы, стоящие перед Казахстаном в области кибербезопасности. Также статья рассматривает развитие технологий обнаружения стеганографических угроз и сотрудничество с международными организациями.*

*Ключевые слова: стеганография, кибербезопасность, Казахстан, защита данных, скрытая информация, цифровая безопасность.*

*Введение:* В эпоху цифровых технологий и развития киберугроз защита информации становится ключевой задачей для любого государства. Казахстан, активно развивающий цифровую экономику и электронное правительство, сталкивается с новыми вызовами в области кибербезопасности. Одним из перспективных инструментов защиты данных является стеганография — метод скрытия информации внутри цифровых объектов. Однако наряду с преимуществами стеганография также используется злоумышленниками для сокрытия вредоносного кода и передачи конфиденциальных данных. В данной статье рассматриваются современные вызовы и возможные решения в области применения стеганографии в кибербезопасности Казахстана.

Стеганография — это метод сокрытия данных в цифровых объектах, таких как изображения, аудиофайлы, видео или сетевые протоколы. В отличие от криптографии, которая скрывает сам смысл сообщения, стеганография скрывает сам факт его существования. Это делает её полезным инструментом как для защиты информации, так и для её несанкционированного использования. Стеганографические методы классифицируются по нескольким основным признакам, таким как тип носителя информации, способ внедрения скрытых данных и уровень сложности обнаружения. По типу носителя информации:

1. Изображения – один из самых популярных носителей для стеганографии. Данные встраиваются в пиксели изображения путем изменения младших битов цветовых компонентов (LSB-метод), изменения частотных характеристик (DCT-метод) или применения пространственных преобразований.

2. Аудиофайлы – используются для сокрытия данных путем незначительного изменения амплитуды звуковых волн или манипуляций с фазами частотных компонентов. Методы включают LSB-стеганографию, фазовое кодирование и скрытие данных в шуме.

3. Видео – скрытие информации происходит аналогично методам стеганографии в изображениях, но с учетом временного измерения, позволяя изменять пиксели в разных кадрах.

4. Текст – стеганография может реализовываться путем изменения пробелов, использования синонимов, перестановки букв или внедрения специальных символов, невидимых для пользователя.

Сетевые протоколы – скрытая передача данных может осуществляться путем изменения заголовков пакетов, использования специфических временных задержек или модификации управляющих сигналов.

По методу внедрения:

1. Замена битов (LSB-метод) – наиболее распространенный способ, при котором изменяются младшие значащие биты пикселей изображения или аудиоданных, что делает изменения практически незаметными.

$$P' = P - (P \bmod 2^n) + m$$

$P$  — исходное значение пикселя,

$P'$  — измененное значение пикселя,  
 $n$  — количество изменяемых бит,  
 $M$  — скрываемая информация (вставляемые биты).

2. Спектральное скрывание – данные маскируются в частотных областях с применением дискретного косинусного преобразования (DCT) или дискретного вейвлет-преобразования (DWT).

$$A_k = \sum_n x(n)\phi(2k - n)$$

$A$  — приближенные сигналы  
 $D$  — детализированные сигналы

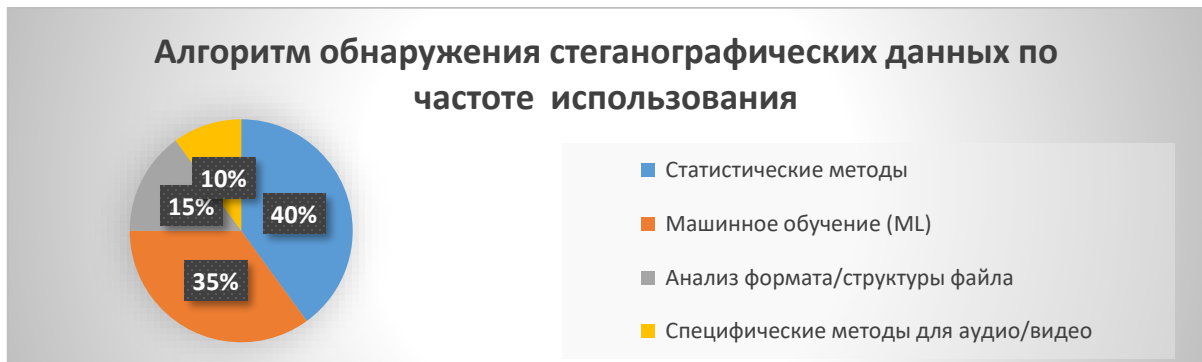
3. Геометрическое преобразование – метод заключается в незначительном изменении формы носителя, например, деформации изображений или варьировании временных параметров в аудиофайлах.

$$\begin{bmatrix} x^1 \\ y^1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} t & y \\ t & x \end{bmatrix}$$

$x, y$  — исходные координаты,  
 $x', y'$  — новые координаты,  
 $a, b, c, d$  — параметры трансформации,  
 $tx, ty$  — смещения.

В сфере кибербезопасности Казахстана стеганография может применяться для:

- Защиты государственных и корпоративных данных;
- Создания цифровых водяных знаков для защиты авторских прав;
- Обеспечения безопасной передачи конфиденциальных данных;
- Обнаружения скрытых угроз и вредоносного кода.



Несмотря на перспективность, стеганография также представляет определенные риски для кибербезопасности Казахстана:

1. Использование стеганографии в кибератаках. Злоумышленники могут использовать стеганографию для сокрытия вредоносных программ в изображениях, аудиофайлах и видео. Это затрудняет обнаружение угроз традиционными антивирусными программами. В 2023 году исследователи в области кибербезопасности обнаружили, что вредоносное ПО может передаваться через обычные медиафайлы, скрывая команды внутри их структуры. В Казахстане в 2022 году была зафиксирована атака на крупную финансовую компанию, когда злоумышленники использовали стеганографию для передачи команд ботнету через изображения, размещённые на легитимных сайтах.

2. Недостаток инструментов для обнаружения стеганографических угроз. В Казахстане недостаточно развито программное обеспечение для выявления стеганографически скрытых данных. Традиционные системы мониторинга сетевого трафика и

антивирусные программы часто не способны идентифицировать скрытые сообщения. Казахстанские банки, такие как Halyk Bank и Kaspi Bank, внедряют системы анализа киберугроз, однако обнаружение стеганографических методов остаётся сложной задачей.

3. Использование стеганографии в финансовых преступлениях. Злоумышленники могут применять стеганографию для обхода систем финансового мониторинга, передавая скрытые команды в цифровых транзакциях или фальсифицируя документы. В 2023 году Агентство финансового мониторинга Казахстана зафиксировало случай, когда преступники скрывали команды для отмыwania денег в зашифрованных изображениях, передаваемых через социальные сети.

В Казахстане есть компании и организации, которые активно работают в области кибербезопасности и внедряют новые технологии для защиты данных:

1. TSARKA — один из ведущих центров по расследованию кибератак, активно занимается анализом новых угроз, в том числе связанных со стеганографией.

2. KZ-CERT — национальный центр киберзащиты, который мониторит угрозы и разрабатывает стратегии борьбы с кибератаками.

3. Kaspi Bank — внедрил технологии искусственного интеллекта для анализа транзакций и предотвращения мошенничества.

4. Halyk Bank — использует системы анализа больших данных для выявления подозрительных финансовых операций. Эти организации играют ключевую роль в обеспечении кибербезопасности Казахстана и могут стать первыми, кто внедрит системы обнаружения стеганографических угроз.

Международный опыт и сотрудничество. Многие страны уже внедрили технологии обнаружения стеганографии для борьбы с киберугрозами. В США, Великобритании и Германии активно развиваются системы машинного обучения, позволяющие анализировать цифровые файлы на предмет скрытых данных. В частности, Национальное агентство безопасности США (NSA) и Центр правительственной связи Великобритании (GCHQ) разрабатывают инструменты для выявления стеганографических атак. Согласно исследованию Европейского агентства по кибербезопасности (ENISA), в 2023 году более 60% кибератак в ЕС использовали методы скрытия данных, включая стеганографию, что вызвало необходимость внедрения новых инструментов мониторинга трафика.

Казахстан активно сотрудничает с международными организациями, такими как INTERPOL и Международный союз электросвязи (ITU), для обмена опытом и разработки стандартов в области борьбы со стеганографией. Казахстан интегрирует свои кибербезопасные структуры, такие как KZ-CERT, в глобальные инициативы по защите цифрового пространства.

На данный момент Казахстан реализует ряд мер, направленных на усиление защиты от киберугроз, включая противодействие стеганографии. Одним из ключевых документов в этой сфере стала Концепция кибербезопасности «Киберщит Казахстана», утвержденная в 2017 году. Она направлена на создание комплексной системы защиты цифрового пространства страны и предотвращение угроз, связанных с кибератаками. В декабре 2023 года был принят закон, вносящий изменения в нормативные акты, регулирующие вопросы информационной безопасности. В нем особое внимание уделяется защите персональных данных и регулированию деятельности в сфере цифрового майнинга. Также в рамках этого закона были инициированы программы по сотрудничеству с экспертами в области кибербезопасности для выявления и устранения уязвимостей в информационных системах.

На международном форуме Digital Almaty 2025 обсуждалось применение технологий искусственного интеллекта в сфере защиты информации. Как отметил глава Комитета по информационной безопасности Министерства цифрового развития, в Казахстане активно внедряется платформа Bug Bounty, а также интегрируются более 220 государственных информационных систем с платформой защиты данных. Эти технологии позволяют

оперативно выявлять уязвимости и предотвращать угрозы, включая методы сокрытия информации с использованием стеганографии. В мае 2024 года было утверждено постановление правительства, определяющее новые требования по обеспечению информационной безопасности. Среди них – использование систем для предотвращения утечек данных (DLP), а также внедрение фильтрации сетевого трафика с применением межсетевых экранов. Эти инструменты повышают уровень защиты от скрытых методов передачи информации.

Таким образом, Казахстан активно совершенствует кибербезопасность, принимая законодательные инициативы, внедряя современные технологии и взаимодействуя с международными организациями.

Стеганография — это мощный инструмент, который может использоваться как для защиты данных, так и в целях кибератак. Для Казахстана важно не только применять стеганографию в области информационной безопасности, но и разрабатывать методы её выявления и предотвращения вредоносного использования. Развитие технологий обнаружения, законодательное регулирование и повышение осведомленности специалистов помогут Казахстану эффективно противостоять киберугрозам, связанным со стеганографией. Внедрение новых технологий и активное сотрудничество государственных и частных компаний в сфере кибербезопасности позволит укрепить цифровую защиту страны и минимизировать риски, связанные с использованием стеганографии в преступных целях.

#### **Список использованных источников:**

1. Кибербезопасность. Учебник для вузов. – Санкт-Петербург: Издательство ЛАНЬ, 2024. – 680 с.
2. Стеганографические методы защиты информации. – Москва: Издательство Каргаслов, 2018. – 250 с.
3. Основы информационной безопасности и стеганографии: учебник и практическое руководство. – Казань: Издательство Казанского федерального университета, 2022. – 295 с.
4. Digital Watermarking and Steganography: Fundamentals and Techniques. – Boca Raton: CRC Press, 2017. – 292 p.

## **WI-FI ЖЕЛІСІНДЕ ШАҚЫРЫЛМАҒАН ҚОНАҚТАРДЫ АВТОМАТТЫ ТҮРДЕ АНЫҚТАУ ЖҮЙЕСІ**

**Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс**

[ttt.ernar@gmail.com](mailto:ttt.ernar@gmail.com), [irgebaikliptonit@gmail.com](mailto:irgebaikliptonit@gmail.com), [salikoalpalpamys@gmail.com](mailto:salikoalpalpamys@gmail.com)

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті, Ақпараттық қауіпсіздік кафедрa студенттері Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс топ 39,39/1

Астана, Қазақстан

Ғылыми жетекшісі – Казиева Н.М.

**Андатпа:** Бұл мақалада Wi-Fi желісіндегі рұқсатсыз қосылған құрылғыларды автоматты түрде анықтау жүйесі қарастырылады. Жүйе желідегі құрылғыларды бақылап, белгісіз MAC-адресстерді сенімді құрылғылар тізімімен салыстырады. Егер рұқсат етілмеген құрылғы анықталса, әкімшіге Telegram API арқылы жедел хабарлама жіберіледі. Python және Scapy құралдарының көмегімен жүзеге асырылған бұл жүйе ARP және DHCP сұраныстарын пайдаланып, желідегі құрылғылардың белсенділігін талдайды. Сонымен қатар, Kali Linux негізінде қауіпсіздік тесттері жүргізіліп, желінің қорғаныс деңгейі бағаланады. Ұсынылған шешім ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға