

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 «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. «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

Зерттеу барысында **NeuVector** жүйесіне бағытталған ықтимал шабуыл векторлары да анықталды. Атап айтқанда, оның сүзу және қорғау механизмдерін айналып өтуге бағытталған шабуылдар талданды. **Kubernetes** пен контейнерлік орталарға қатысты белгілі **CVE** осалдықтарын зерттеу кешенді қауіпсіздік тәсілін қолданудың маңыздылығын растады. Бұл тәсіл желілік трафикті мінез-құлықтық талдауды және қауіптерге проактивті ден қоюды қамтуы тиіс.

Осылайша, **NeuVector Kubernetes** кластерлерінің қауіпсіздігін күшейтуге арналған маңызды құрал болып табылады. Дегенмен, оны басқа қауіпсіздік әдістерімен үйлестіре отырып қолдану қажет. Болашақ зерттеулердің бағыттары ретінде машиналық оқытуға негізделген автоматтандырылған шабуылдарды анықтау жүйелерін әзірлеу және контейнерлік орталарға арналған **Threat Intelligence** модельдерін жетілдіру қарастырылады.

Қолданылған әдебиеттер тізімі

1. **Red Hat.** State of Kubernetes Security Report, 2024. Сілтеме: <https://www.redhat.com/en/engage/state-kubernetes-security-report-2024>.
2. **State of Kubernetes Security Report, 2024.** Сілтеме: https://static.carahsoft.com/concrete/files/3616/8252/7918/3-4_State_of_Kubernetes_Security_Report.pdf
3. **Дарвеш Г., Хаммуд Д., Воробьева А. А.** Security in Kubernetes: best practices and security analysis // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2 (44). – С. 63-69.
4. **Rostami G.** Role-based access control (RBAC) authorization in Kubernetes // Journal of ICT Standardization. – 2023. – Т. 11. – № 3. – С. 237-260.
5. **Muslim A., Recker S.** Controller-Based Admission Control for Containers // 2024 IEEE International Conference on Cloud Engineering (IC2E). – IEEE, 2024. – С. 34-43.
6. **German K., Ponomareva O.** An overview of container security in a Kubernetes cluster // 2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT). – IEEE, 2023. – С. 283-285.
7. **Cabianca D.** Managing Security Operations // Google Cloud Platform (GCP) Professional Cloud Security Engineer Certification Companion: Learn and Apply Security Design Concepts to Ace the Exam. – Berkeley, CA : Apress, 2024. – С. 433-566.
8. **NeuVector Documentation.** Сілтеме: <https://open-docs.neuvector.com/>.
9. **Sadiq A. et al.** Detection of denial of service attack in cloud-based Kubernetes using eBPF // Applied Sciences. – 2023. – Т. 13. – № 8. – С. 4700.
10. **Red Hat Security Advisory.** CVE-2024-9042. Сілтеме: <https://access.redhat.com/security/cve/cve-2024-9042>.
11. **Red Hat Security Advisory.** CVE-2024-9486. Сілтеме: <https://access.redhat.com/security/cve/cve-2024-9486>.
12. **NeuVector Release Notes 5.x.** Сілтеме: <https://open-docs.neuvector.com/5.2/releasenotes/5x>.
13. **SUSE Security Advisory.** CVE-2024-24791. Сілтеме: <https://www.suse.com/security/cve/CVE-2024-24791.html>.

УДК 004.056.55

СТЕГАНОГРАФИЯ НА ОСНОВЕ LSB: РЕАЛИЗАЦИЯ СОКРЫТИЯ ДАННЫХ В МЕДИАФАЙЛАХ

Жанатаев Мирас Куанышевич

Kmiras212@gmail.com

Студент Факультета информационных технологий по специальности: системы информационной безопасности ЕНУ им. Л. Н. Гумилева, Астана, Казахстан
Научный руководитель - Шахметова. Г. Б.

Введение в стеганографию

Стеганография — это довольно древнее и увлекательное искусство сокрытия информации внутри другой части информации, то есть создание секретного канала связи, который остается невидимым для случайных наблюдателей [1]. В отличие от криптографии, которая шифрует сообщение чтобы сделать его нечитаемым, стеганография направлена на то, чтобы полностью скрыть существование самого сообщения. Представьте, что вы пишете сообщение на листе бумаги, а затем встраиваете его в ткань ковра таким образом, что никто и не заподозрит о его присутствии - в этом вся суть стеганографии.

На протяжении всей истории люди использовали хитроумные методы сокрытия сообщений: невидимые чернила, микроточки, скрытые татуировки и даже надписи, вшитые в одежду. В эпоху цифровых технологий стеганография эволюционировала, чтобы использовать современные медиа, такие как изображения, аудиофайлы и видео, для передачи секретной информации.

Метод встраивание в наименее значимые биты (LSB)

Среди различных методов цифровой стеганографии метод LSB выделяется своей простотой и эффективностью [2]. По своей сути, стеганография LSB использует тот факт, что крошечные изменения в цифровых данных часто незаметны человеческому восприятию.

В цифровых данных данные представлены в двоичном виде (битами). Например, в 8-битном представлении цветового или звукового сэмпла старшие биты (крайние левые) определяет основные характеристики данных, в то время как младшие биты (крайние правые) представляют незначительные изменения, которые обычно не заметны. Метод LSB работает путем замены этих наименее значимых битов на биты.

- В изображении изменение последнего бита значения цвета пикселя может изменить его интенсивность всего на $1/255$, что незаметно невооруженным глазом.
- В аудиофайле изменение наименее значимых битов звуковых сэмплов создает незаметный шум.

Практический пример:

Будет рассмотрен пиксель со значением RGB (200,150,100). В двоичном формате это выглядит следующим образом:

- Красный: 11001000
- Зеленый: 10010110
- Синий: 01100100

Для того, чтобы скрыть бинарное сообщение "10", необходимо изменить исходные данные таким образом:

- Красный: 11001001
- Зеленый: 10010111
- Синий: 01100101

Были скрыты два бита информации, но визуальная разница совершенно незаметна.

Анализ программной реализации:

Программа реализована на Python, демонстрирует надежный подход к стеганографии (LSB) с добавлением шифрования для повышенной безопасности.

Реализация поддерживает два типа медиафайлов для скрытия сообщений:

Аудио стеганография (WAV, MP3 - форматы)

1. Преобразует зашифрованное сообщение в двоичную строку.
2. Изменяет младший бит каждого аудио кадра.
3. Позволяет скрывать сообщения в звуковых файлах с минимальным ухудшением качества звука.

Стеганография изображений (PNG, JPEG)

1. Изменяет младший бит цветового канала.
2. Поддерживает различные форматы изображений, сохраняя визуальную целостность.

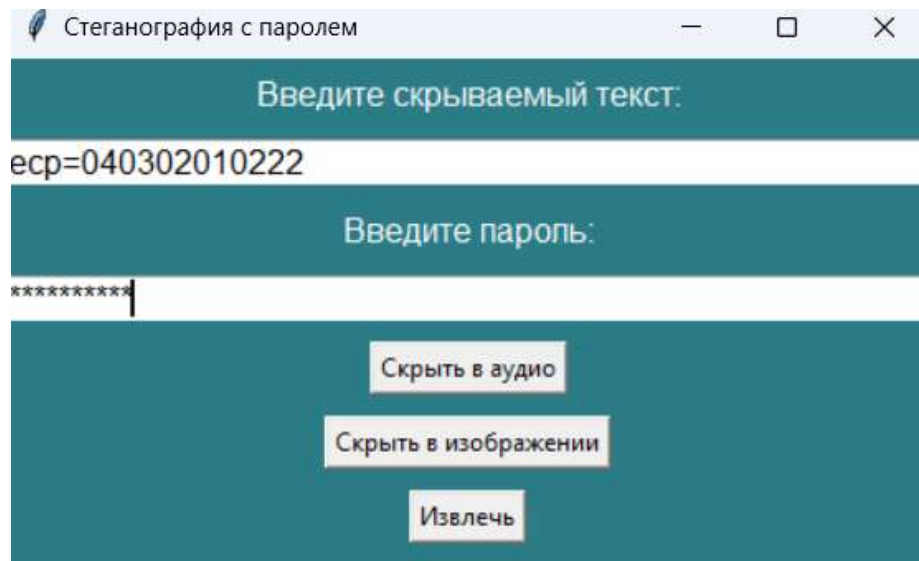


Рис.1 – Графический интерфейс приложения

В самом графическом интерфейсе можно ввести скрываемый текст по указанному полю, а также и пароль для двухэтапной безопасности. По перечисленным кнопкам на [Рис.1] можно выбрать тип файла в которой будет скрываться сообщение, аудио-формат, изображение или видео. Прежде чем скрыть сообщение, программа его шифрует с помощью шифрование AES-256. Это двухэтапный процесс обеспечивает несколько уровней безопасности: сначала сообщение шифруется, защищая его содержимое. Затем зашифрованное сообщение скрывается с помощью стеганографии методом LSB.

Функция `derive_key()` использует SHA-256 для генерации 32-байтового ключа на основе предоставленного пользователем пароля [Рис.2]. Это гарантирует, что даже при использовании одного и того же пароля при каждом шифровании создается уникальный ключ.

```
280 def derive_key(password: str) -> bytes: 2 usages
281     return hashlib.sha256(password.encode()).digest()
```

Рис.2 – Функция шифрования

Приступим к сокрытию конфиденциальной информации:

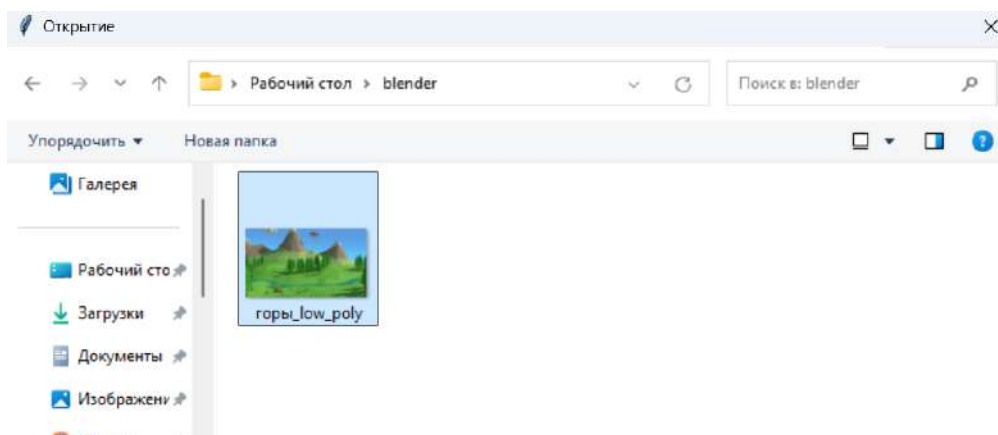


Рис.3 – Выбранная картинка с расширением PNG

После того как был выбран файл, в нашем случае PNG – изображения [Рис.3], выйдет новое окно с информацией об успешной операции, либо с ошибкой [Рис.4]. Файл со скрытым сообщением создан в той директории, где хранился исходный файл.

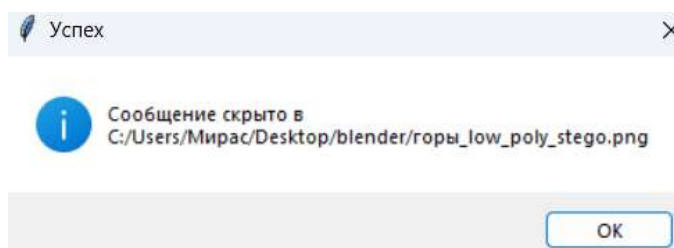


Рис.4 – Окно с успешным внедрением скрытого сообщения

По [Рис.5] видно, что размеры файлов отличаются всего на 18 кбит, это означает что наш файл не вызовет подозрение от третьих лиц, также видим, что он сохранился в таком же формате что и исходный файл.

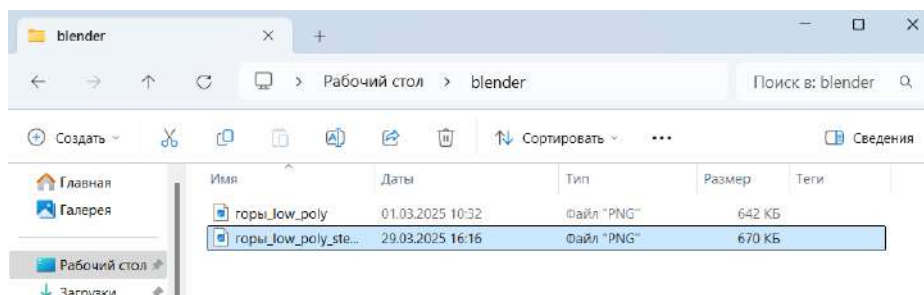


Рис.5 – Различие размеров между исходным и измененным файлом



Рис.6 – Визуальное различие между файлами (слева – исходное, справа - измененное)

На первый взгляд, снимки идентичны – пиксели, цвета и композиция совпадают полностью. Однако в изображении справа информация спрятана в младших битах цветовых каналов пикселей, создавая тонкие изменения, который можно обнаружить только специальными алгоритмами стеганографического анализа [Рис.6].

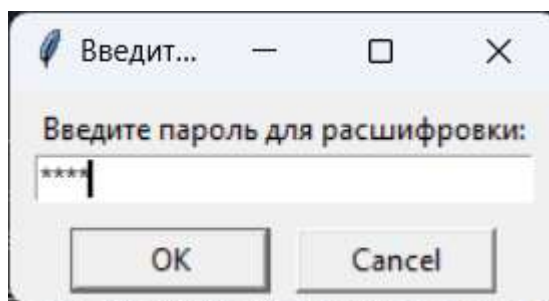


Рис.7 – Поле ввода пароля для расшифровки файла

Для декодирования измененного изображения нам нужно выбрать операцию извлечь из [Рис.1]. Выбрать сам измененный файл и прописать пароль чтобы получить доступ к скрытому сообщению [Рис.7].

Процесс декодирования обращает обратно модификацию LSB: извлекает младшие биты из медиакадров/пикселей, восстанавливает двоичное сообщение. Расшифровывает сообщение, используя предоставленный пароль [Рис.8].

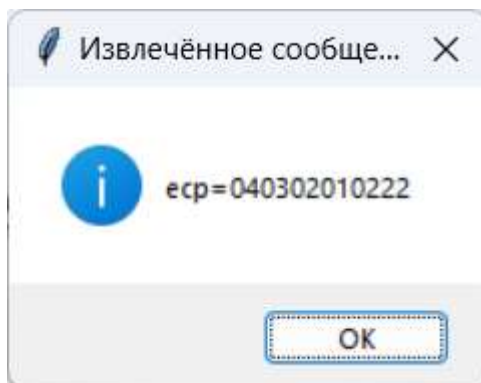


Рис.8 – расшифрованное сообщение

Список используемых источников

1. Fridrich J., Goljan M. Practical steganalysis of digital images: state of the art //security and Watermarking of Multimedia Contents IV. – 2002. – Т. 4675. – С. 1-13.
2. Singh A. K., Singh J., Singh H. V. Steganography in images using LSB technique //International Journal of Latest Trends in Engineering and Technology (IJLTET). – 2015. – Т. 5. – №. 1. – С. 426-430.
3. NumPy. Официальная документация. URL: <https://numpy.org/doc/2.2/> (дата обращения: 28.03.2025)
4. Python. Официальная документация. URL: <https://docs.python.org/3/> (дата обращения: 28.03.2025)
5. Provos N., Honeyman P. Hide and seek: An introduction to steganography //IEEE security & privacy. – 2003. – Т. 1. – №. 3. – С. 32-44.