

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. «EDSAFE 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

контроль сетевого взаимодействия (например, с помощью eVRF или iptables) и чёткое понимание цели их использования.

Заключение

В ходе настоящего исследования продемонстрирована высокая эффективность использования honeypot-систем как инструмента проактивной защиты информационных систем. На основе экспериментальных данных показано, что даже с минимальными затратами можно получить ценную информацию о текущих атаках, применяемых инструментах и поведении злоумышленников. Это делает honeypot-системы важным элементом современной архитектуры кибербезопасности, наряду с SIEM, NIDS и системами анализа поведения. Результаты работы могут быть полезны специалистам по информационной безопасности при проектировании систем обнаружения атак, формировании стратегии киберразведки и разработке обучающих платформ для подготовки кадров SOC-центров.

Список использованных источников

1. Spitzner L. Honeypots: Tracking Hackers. Addison-Wesley, 2002.
2. Provos N., Holz T. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley, 2007.
3. Mokube I., Adams M. Honeypots: Concepts, Approaches, and Challenges // Proceedings of the 45th ACM Southeast Conference. ACM, 2007.
4. Танкелевич В. Системы-ловушки (Honeypots) как инструмент повышения уровня защищенности информационных систем // Информационная безопасность, №1, 2019.
5. Cowrie Honeypot Project. URL: <https://github.com/cowrie/cowrie>
6. Dionaea Honeypot. URL: <https://github.com/DinoTools/dionaea>

УДК 004.056:614.2

АНАЛИЗ РИСКАМИ БЕЗОПАСНОСТИ ДАННЫХ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Нуриева Дана Робертовна

nurievadana5@gmail.com

[Исайнова Алия Насиповна](#)

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Аннотация

Предмет. В последние годы цифровизация здравоохранения значительно ускорила процессы обработки и хранения медицинских данных. Медицинские учреждения все чаще используют электронные информационные системы, облачные платформы и технологии дистанционного медицинского обслуживания. Однако вместе с этим значительно возросли и риски утечек, несанкционированного доступа и кибератак на базы данных пациентов.

Медицинская информация является крайне чувствительной, поскольку содержит персональные данные, историю болезней, результаты анализов и другие сведения, которые могут использоваться злоумышленниками в преступных целях, включая мошенничество, шантаж и незаконную продажу данных. Казахстан, активно развивающий сферу цифровой медицины, столкнулся с необходимостью усиления мер по обеспечению кибербезопасности в медицинских учреждениях. Государственная система «Дамумед», предназначенная для автоматизации медицинских процессов, подверглась критике за уязвимости, что подчеркивает необходимость совершенствования системы защиты данных.

Актуальность исследования обусловлена потребностью в системном анализе существующих угроз, выявлении слабых мест в системе безопасности медицинских учреждений и разработке эффективных подходов к управлению рисками. Это особенно важно в контексте развития законодательных и нормативных требований в Казахстане и приведения системы защиты данных в соответствие с международными стандартами.

Цели. Комплексным авторским исследованием являются системы управления рисками информационной безопасности в медицинских учреждениях Казахстана.

Предмет исследования. Механизмы выявления, анализа и минимизации угроз, направленных на компрометацию медицинских данных, а также способы адаптации международных стандартов к казахстанским условиям.

Методология. Исследование основано на сочетании нескольких методологических подходов:

- Онтологический анализ позволяет определить и систематизировать ключевые понятия, связанные с информационной безопасностью медицинских данных, а также разработать структуру классификации угроз и уязвимостей;
- Сравнительный анализ применяется для сопоставления казахстанской системы «Дамумед» с зарубежными медицинскими информационными системами, выявления различий в подходах к обеспечению безопасности данных;
- Системный анализ используется для изучения структуры угроз, взаимосвязи факторов риска и последствий их реализации;
- Аналитический обзор литературы позволяет выявить основные тенденции в развитии информационной безопасности медицинских учреждений и интеграции нормативных стандартов;
- Методы количественной оценки рисков применяются для расчета потенциальных угроз и вероятности их реализации.

Научная новизна заключается в комплексном изучении проблематики кибербезопасности медицинских учреждений Казахстана, адаптации международных стандартов к отечественным условиям и разработке модели управления рисками, ориентированной на национальную систему здравоохранения.

Результаты.

Таблица 1

Классификация ключевых понятий кибербезопасности медицинских данных

Термин	Определение	Применение в кибербезопасности медицины
Доступность	Гарантия того, что данные доступны уполномоченным лицам в нужный момент	Обеспечение работы медицинских информационных систем в экстренных ситуациях
Целостность	Защита информации от несанкционированных изменений и подделок	Предотвращение модификации медицинских записей, защита от атак на базы данных
Киберугрозы	Потенциальные атаки на информационные системы, направленные на кражу, модификацию или уничтожение данных	Фишинг, ransomware, DDoS-атаки, уязвимости в ПО
Уязвимости	Слабые места в системе, которые могут быть использованы злоумышленниками	Ошибки в коде, устаревшие системы, недостаточная подготовка персонала

Управление рисками	Анализ угроз, оценка вероятности атак, разработка мер реагирования	Внедрение стандартов безопасности (ISO 27001, NIST), мониторинг кибератак
Источник: [1 - 4]		

Как показано в Таблице 1, ключевые понятия кибербезопасности медицинских данных включают конфиденциальность, доступность и целостность (CIA-триада), а также управление рисками и киберугрозы. Однако, в отличие от международных стандартов, в казахстанских исследованиях большее внимание уделяется техническим аспектам защиты, а не адаптивности системы к возможным атакам и стратегиям восстановления данных. Это указывает на необходимость дальнейшей интеграции международных стандартов, таких как NIST Cybersecurity Framework и ISO 27001, в национальную практику кибербезопасности, что позволит обеспечить не только защиту, но и устойчивость медицинских информационных систем к современным угрозам.

Как следует из данных Таблицы 2, элементы зарубежных стандартов реализуются преимущественно в государственных учреждениях, тогда как частный сектор зачастую остаётся вне рамок строгого регулирования. Для формирования полноценной системы информационной безопасности в здравоохранении требуется усиление институциональных механизмов, развитие программ подготовки специалистов, гармонизация законодательства с глобальными нормами и создание национальных механизмов сертификации, что обеспечит устойчивость и доверие к цифровым медицинским сервисам.[5-6]

Таблица 2

Сравнительная характеристика международных стандартов кибербезопасности в медицине.

Стандарт	Основные положения	Применение в здравоохранении	Адаптация в Казахстане
ISO/IEC 27001	Комплексная система управления информационной безопасностью (ISMS), включает идентификацию рисков, контроль доступа, меры по защите данных, шифрование и аудит безопасности	Используется для защиты электронных медицинских карт, систем хранения данных пациентов, а также контроля над доступом к медицинской информации	Внедряется в крупных медицинских учреждениях, однако сертификация сложна и требует значительных финансовых затрат для частных клиник
НПРАА	Обеспечение конфиденциальности пациентов, строгий контроль доступа, требования к шифрованию данных, обязательные меры по аудиту и мониторингу	Применяется операторами медицинской информации, больницами, страховыми компаниями и провайдерами электронных медицинских записей в США	Частично адаптирован в Казахстане – используется шифрование данных и многофакторная аутентификация, но на законодательном уровне нет четких требований к соблюдению НПРАА
NIST Cybersecurity Framework	Комплексный подход к управлению киберрисками, включает выявление угроз, защиту данных, мониторинг атак, реагирование и восстановление системы	Используется для защиты медицинских систем, раннего обнаружения атак, разработки планов реагирования на инциденты	Отдельные принципы применяются в государственных клиниках, особенно в сфере мониторинга угроз и реагирования на инциденты

Архитектура системы «Дамумед» построена по клиент-серверной модели, что обеспечивает гибкость, масштабируемость и отказоустойчивость платформы. Центральной частью системы является серверная инфраструктура, включающая в себя централизованную базу данных, серверы приложений, модули безопасности и распределенные точки доступа.

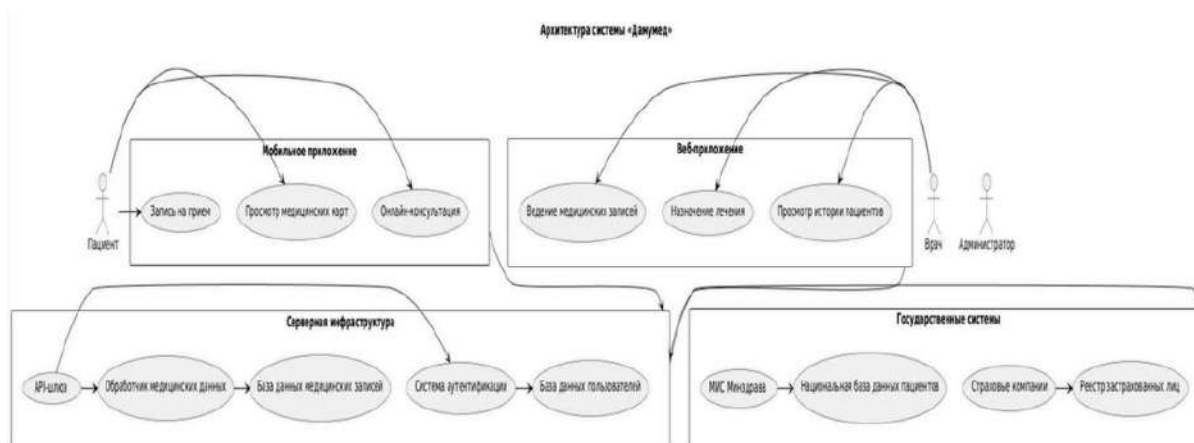


Рисунок 1 Схема архитектуры системы «Дамумед».

Таблица 3

Основные угрозы безопасности в системе «Дамумед» и методы защиты

Тип угрозы	Описание	Методы защиты
Фишинговые атаки	Злоумышленники рассылают поддельные письма или создают фальшивые сайты, чтобы украсть учетные данные пользователей	Обучение персонала, двухфакторная аутентификация (2FA), фильтрация подозрительных e-mail
Программы-вымогатели (ransomware)	Шифрование данных с требованием выкупа за их восстановление	Регулярное резервное копирование, антивирусный контроль, защита доступа к серверу
Уязвимости в мобильном приложении	Недостаточная защита API-интерфейсов может привести к утечке данных через мобильное соединение	Использование шифрования TLS 1.3, проверка безопасности API, аудит кода
DDoS-атаки	Массовые запросы перегружают серверы, делая систему недоступной	Защита от перегрузок, автоматическое масштабирование, фильтрация трафика
Инсайдерские угрозы	Сотрудники или медицинский персонал могут умышленно передавать конфиденциальные данные	Контроль доступа, ведение логов активности пользователей, мониторинг подозрительных действий
Примечание: Составлено автором в результате исследования.		

Как показано в Таблице 3, для повышения уровня безопасности «Дамумед» необходимо развивать защитные механизмы мобильного приложения, усиливать мониторинг активности пользователей, внедрять дополнительные алгоритмы шифрования и повышать уровень цифровой грамотности медицинского персонала. Дальнейшая модернизация системы и адаптация международных стандартов кибербезопасности позволят существенно снизить риски несанкционированного доступа и обеспечить надежную защиту медицинских данных пациентов.

Таблица 4
Основные функциональные различия «Дамумед» и зарубежных систем

Система	ЭМК	Телемедицина	Интеграция с госструктурами	Мобильные приложения	Аналитика и прогнозирование
<i>Дамумед (Казахстан)</i>	Поддержка интеграция с ЭМК гос. структурами	Ограниченный функционал	Подключение к нац. базам	Есть мобильное приложение	Ограниченный функционал
<i>EPIC (США)</i>	Полнофункциональные ЭМК	Развитая телемедицина	Ограничено	Поддержка мобильных устройств	ИИ-аналитика
<i>Cerner (США)</i>	Гибкая настройка ЭМК	Встроенные телемедицинские сервисы	Ограничено	Поддержка приложений	Прогнозирование на основе данных
<i>Allscripts (США, ЕС)</i>	Ориентация на частные клиники	Поддержка удаленных консультаций	Ограничено	Упор на мобильные сервисы	Анализ медицинских данных
<i>NHS Digital (Великобр.)</i>	Государственная база ЭМК	Полная интеграция с NHS	Полная интеграция	Интеграция с NHS-приложениями	Использование AI-решений
<i>Meditech (США, Канада)</i>	Простая интеграция с другими системами	Базовая телемедицина	Нет	Базовая поддержка	Базовый анализ

Анализ сравнительных характеристик показывает, что система «Дамумед» по ряду ключевых направлений — в частности, в области телемедицины, интеллектуального анализа данных и внедрения прогностических инструментов — отстает от признанных международных решений, таких как EPIC, Cerner или NHS Digital. Зарубежные платформы активно применяют искусственный интеллект, машинное обучение и предиктивную аналитику для раннего выявления заболеваний, персонализированного лечения и повышения эффективности управленческих решений. В то же время функционал «Дамумед» в этих аспектах пока ограничен и требует дальнейшего развития. Это ограничивает потенциал системы в части интеграции с современными сервисами цифрового здравоохранения и сдерживает ее адаптацию к быстро меняющимся условиям медицинской практики в эпоху глобальной цифровизации.[10]

Совершенствование кибербезопасности медицинских информационных систем требует интеграции организационных, технических и правовых решений. Ключевыми направлениями являются: Внедрение политик информационной безопасности и обучение персонала; Использование современных технологий: шифрование (AES-256, RSA), многофакторная аутентификация (MFA), SIEM-системы; Адаптация международных стандартов (GDPR, HIPAA, ISO/IEC 27001) в казахстанскую практику.

Закключение. В процессе исследования была проведена всесторонняя оценка текущего состояния кибербезопасности в медицинских учреждениях Казахстана. Выявлены ключевые угрозы, такие как фишинговые атаки, уязвимости мобильных приложений и недостаточная защита облачных решений. Сравнительный анализ показал, что система «Дамумед» уступает зарубежным аналогам по уровню защиты данных и соответствию международным стандартам. Адаптация ISO/IEC 27001, HIPAA и GDPR в условиях Казахстана требует модернизации нормативной базы, развития ИТ-инфраструктуры и подготовки профильных специалистов. Для повышения уровня киберустойчивости предложены конкретные меры: внедрение многофакторной аутентификации, использование современных алгоритмов шифрования, развитие SIEM-систем и обучение персонала. Особое внимание уделяется перспективным технологиям — искусственному интеллекту, блокчейну и облачным платформам, способным существенно усилить защиту данных пациентов. Полученные выводы могут быть использованы для выработки государственной стратегии информационной безопасности и дальнейших научных исследований в сфере цифрового здравоохранения.

Список использованных источников

1. Nowrozy R., Ahmed K. Enhancing health information systems security: An ontology model approach // International Conference on Health Information. – 2023. – https://link.springer.com/chapter/10.1007/978-981-99-7108-4_8.

2. Mozzaquatro B.A., Agostinho C., Goncalves D., Martins J. An ontology-based cybersecurity framework for the internet of things // Sensors. – 2018. – <https://www.mdpi.com/1424-8220/18/9/3053>.
3. Hannou F.Z., Atigui F., Lammari N., Cherfi S.S. SafecareOnto: A cyber-physical security ontology for healthcare systems // International Conference on Advanced Information Networking and Applications. – 2021. – https://link.springer.com/chapter/10.1007/978-3-030-86475-0_3.
4. Arunprasath S., Annamalai S. Improving patient-centric data retrieval and cybersecurity in healthcare: privacy-preserving solutions for a secure future // Multimedia Tools and Applications. – 2024. – <https://link.springer.com/article/10.1007/s11042-024-18253-5>.
5. Harris S., Liu J., Ta V.T., Hadi H.J., Khan A., Zukaib U. Cybersecurity Standards for AI-based Healthcare Networks // ResearchGate. – 2023. – https://www.researchgate.net/publication/385622651_Cybersecurity_Standards_for_AI_based_Healthcare_Networks.
6. Singh G.P., Bharti V., Hooda M.K. A Review on NIST, ISO 27001, HIPAA and MITRE ATT&CK Cybersecurity Frameworks // Webology. – 2021. – https://www.researchgate.net/publication/371313513_A_Review_on_NIST_ISO_27001_HIPAA_and_MITRE_ATTCK_Cybersecurity_Frameworks.

УДК 004.056

КЕСКІНДЕРДЕГІ СТАТИСТИКАЛЫҚ СТЕГОАНАЛИЗ ӘДІСТЕРІ

Нұрлан Айсұлу Таңатқызы

nurlanaisulu19@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті
Ақпараттық қауіпсіздік жүйелері кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекші – Онгарбаева Айнагуль Игиликовна

Андатпа. Бұл мақалада кескіндердегі статистикалық стегоанализдеу әдістері қарастырылады. Сонымен қатар, қазіргі стеганализ алгоритмдері мен әдістерінің жұмыс істеу принциптері берілген. Әртүрлі стеганализ әдістерінің тиімділігіне және олардың шектеулеріне көп көңіл бөлінеді. Кескіндегі жасырын ақпаратты анықтаудағы статистикалық стегоанализдің әдістеріне төменгі биттік талдау, хи-квадрат әдісі, RS талдауы және тағы да басқа әдістер жұмыста көрсетілген.

Кілт сөздер: стеганография, стегоанализ, статистикалық стеганография, статистикалық стегоанализ, кескіндерді талдау, жасырын ақпарат, пиксельдер, ақпараттық қауіпсіздік.

Кіріспе

Стеганография - бұл деректердің ішінде құпия ақпараттың болуын анықтауды мүмкін емес ететіндей оны жасыру туралы ғылым. Статистикалық стеганография мәліметтерді кескіндер, аудио файлдар және мәтіндік құжаттар сияқты деректерді өзгеріссіз цифрлық тасымалдаушыларға енгізуді білдіреді. Құпия хабарламалар саласында стеганографияның бірнеше негізгі әдістері бар. Олардың ішінде статистикалық стеганография әдіс ақпаратты енгізу процесінен кейінгі статистикалық өзгерістерді барынша көрінбейтіндей етіп жасырады.

Стеганографияның дамуымен бірге оған қарама-қарсы стегоанализ әдістері де жетілдірілуде. Оның мақсаты - цифрлық медида жасырын ақпараттың болу фактісін анықтау. Стегоанализ жасаудың әртүрлі тәсілдер бар, ең кең таралған және тиімдісі статистикалық стеганализ болып табылады. Өйткені ол статистикалық сипаттамаларға негізделген және ең