

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

**Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖАҢЕ БІЛІМ - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ҒЫЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ҒЫЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

**«GYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың
XX Халықаралық ғылыми конференциясы = XX Международная
научная конференция студентов и молодых ученых «GYLYM JÁNE
BILIM – 2025» = The XX International Scientific Conference for
students and young scholars «GYLYM JÁNE BILIM – 2025». – Астана:
– 3813 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-08-5373-7

**Жинаққа студенттердің, магистранттардың, докторанттардың және жас
ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті
мәселелері бойынша баяндамалары енгізілген.**

**The proceedings are the papers of students, undergraduates, doctoral students and young
researchers on topical issues of natural and technical sciences and humanities. В сборник
вошли доклады студентов, магистрантов, докторантов и молодых ученых по
актуальным вопросам естественно-технических и гуманитарных наук.**

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған ai дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «ИОТ Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
Подсекция 2.4		
Информационная безопасность		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «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., Қайулов 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. Рамагуллаев 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

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ РАЗРАБОТЧИКОВ С ПОМОЩЬЮ ИНТЕГРИРОВАННЫХ ИСКУССТВЕННЫХ ИНТЕЛЛЕКТОВ И СООБРАЖЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Сергазы Мэди

saitamenter@gmail.com

Кафедра систем информационной безопасности, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан

Научный руководитель – PhD, старший преподаватель Токseit Динара

Аннотация

Стремительное развитие искусственного интеллекта (ИИ) привело к появлению новых инструментов для повышения производительности разработчиков, особенно в области кибербезопасности. Cursor AI, помощник по программированию на базе искусственного интеллекта, предназначен для оптимизации разработки программного обеспечения путем предоставления предложений по коду в режиме реального времени, поддержки отладки и повышения безопасности. В этом обзоре рассматривается влияние разработки Cursor AI on, ориентированной на кибербезопасность, подчеркивается ее роль в повышении эффективности, сокращении количества ошибок и внедрении методов безопасного кодирования. В статье рассматриваются существующие помощники по кодированию, управляемые ИИ, сравниваются их функциональные возможности и оценивается уникальный вклад Cursor AI в разработку безопасного программного обеспечения. Кроме того, обсуждаются потенциальные риски, связанные с кодированием с помощью ИИ, и предлагаются стратегии снижения рисков для обеспечения надежности и безопасности.

Кибербезопасность остается серьезной проблемой, поскольку уязвимости программного обеспечения продолжают развиваться. Традиционные методы программирования требуют тщательной отладки и аудита безопасности, что делает разработку программного обеспечения трудоемким и сложным процессом. Помощники по программированию на базе искусственного интеллекта, такие как Cursor AI, меняют мир, предлагая интеллектуальные рекомендации, выявляя угрозы безопасности и помогая в отладке. Эти инструменты помогают разработчикам более эффективно писать защищенный код, снижая вероятность человеческой ошибки и повышая общую целостность программного обеспечения.

В этой статье рассматривается, как Cursor AI помогает разработчикам писать более безопасный код, сокращая количество ошибок, повышая осведомленность о безопасности и ускоряя процесс разработки. Кроме того, в ней оцениваются потенциальные риски и этические проблемы, связанные с кодом, созданным с помощью искусственного интеллекта, что гарантирует, что такие инструменты остаются активами, а не обязательствами при разработке безопасного программного обеспечения.

Cursor AI интегрируется с широко используемыми средами разработки и обеспечивает поддержку разработчиков в режиме реального времени. Он обеспечивает интеллектуальное автозавершение, помогая программистам писать более точный код, сводя к минимуму синтаксические и логические ошибки. Инструмент также обладает возможностями автоматической отладки, что позволяет разработчикам быстрее выявлять и устранять проблемы. Помимо повышения производительности, Cursor AI способствует повышению

безопасности кодирования, выявляя потенциальные уязвимости и предлагая рекомендации, основанные на установленных рекомендациях по кибербезопасности. Эта функциональность делает его особенно полезным в приложениях, чувствительных к безопасности, где важна точность.

Существует несколько программных ассистентов на базе искусственного интеллекта, в том числе GitHub Copilot и Tab nine, каждый из которых обладает уникальными функциями. Хотя эти инструменты предлагают общую поддержку автозавершения и кодирования, Cursor AI выделяется своей ориентацией на безопасность. Он содержит предложения, соответствующие принципам безопасного программирования, интегрируется с системами кибербезопасности и предлагает рекомендации, основанные на лучших практиках, таких как те, которые описаны Фондом OWASP. Эти функции делают Cursor AI ценным ресурсом для разработчиков, работающих над проектами, критически важными для безопасности.

Риски

Хотя инструменты, основанные на искусственном интеллекте, такие как Cursor AI, значительно улучшают разработку программного обеспечения и кибербезопасность, их использование сопряжено с определенными рисками и проблемами. Одной из основных проблем является потенциальное наличие скрытых уязвимостей в коде, созданном с помощью искусственного интеллекта. Несмотря на то, что инструменты ИИ разработаны таким образом, чтобы свести к минимуму человеческие ошибки, они все равно могут упускать из виду незначительные недостатки или создавать слабые места, которые трудно обнаружить. Эти уязвимости могут быть особенно опасны в приложениях, требующих обеспечения безопасности, где небольшая ошибка может привести к крупномасштабным нарушениям. Еще одной проблемой является чрезмерная зависимость от ИИ. По мере того как инструменты ИИ становятся все более мощными, разработчики могут начать доверять им слишком сильно, что приведет к сокращению ручного контроля.

Такая зависимость от ИИ при генерации кода может привести к самоуспокоенности при проверке кода вручную, что потенциально может позволить критическим недостаткам безопасности остаться незамеченными. Разработчики также могут стать менее квалифицированными в выявлении основных проблем в коде, поскольку они могут не принимать активного участия в отладке. Этические проблемы также возникают с такими инструментами искусственного интеллекта, как Cursor AI, поскольку они часто извлекают уроки из обширных наборов данных общедоступного кода, что вызывает опасения по поводу интеллектуальной собственности и авторских прав. Эти инструменты могут непреднамеренно генерировать код, похожий на запатентованный материал, что может привести к юридическим последствиям. Кроме того, предложения, сгенерированные с помощью искусственного интеллекта, могут отражать искажения, присутствующие в обучающих данных, что влияет на честность и доступность сгенерированного кода. Наконец, интеграция ИИ с существующими системами является сложной задачей, особенно для устаревших кодовых баз. Инструменты ИИ, как правило, разрабатываются с учетом современных языков программирования и сред, и их интеграция в более старые системы может привести к проблемам совместимости или неэффективности. Разработчикам может потребоваться дополнительное обучение или ресурсы, чтобы в полной мере использовать эти инструменты в таких средах.

Потенциальные разработки в будущем

Заглядывая в будущее, можно сказать, что потенциал ИИ в разработке программного обеспечения и кибербезопасности огромен. В ближайшем будущем могут появиться инструменты ИИ, такие как Cursor AI, которые будут автоматически обнаруживать новые и ранее невиданные уязвимости, постоянно извлекая уроки из расширяющегося спектра угроз

безопасности. По мере совершенствования моделей ИИ они смогут обнаруживать не только известные уязвимости, но и выявлять закономерности, указывающие на новые атаки. Одной из интересных возможностей является интеграция инструментов ИИ в рабочие процессы DevSecOps (разработка, безопасность и эксплуатация). Искусственный интеллект может стать ключевым компонентом конвейеров CI/CD (Continuous Integration/Continuous Deployment), автоматически сканируя и защищая код по мере его написания. Это позволит обнаруживать уязвимости в режиме реального времени во время работы разработчиков, что значительно сократит время, необходимое для устранения проблем, и повысит общую безопасность программного обеспечения. Более того, по мере того, как инструменты искусственного интеллекта будут понимать контекст кода, они смогут вносить более разумные предложения и даже самостоятельно устранять неполадки, предоставляя разработчикам комплексные решения сложных задач. Например, ИИ может быть способен переработать большую часть небезопасного кода и предложить рекомендации по улучшению архитектуры для повышения устойчивости к угрозам безопасности. Этический ИИ также станет важным направлением. В будущем разработка ИИ будет включать в себя более надежные системы для обеспечения прозрачности и подотчетности в коде, созданном с помощью ИИ. Эти достижения будут иметь важное значение для решения таких проблем, как интеллектуальная собственность, предвзятость и потенциальное злоупотребление искусственным интеллектом при создании вредоносного кода.

Таблица 1. Сравнение помощников по кодированию на базе искусственного интеллекта

Feature	Cursor AI	GitHub Copilot	Tabnine
Natural Language Commands	Yes	Limited	Yes
Agent Mode/Composer	Yes	Yes, Edits feature	No
Privacy Mode	Yes	No explicit privacy mode mentioned	Yes
Integration with Security Tools	Yes, e.g., Aikido Security	Limited information	No
Security Features	Secure coding practices aligned with OWASP	Basic security suggestions	General code assistance

GitHub Copilot, работающий на базе OpenAI Codex, является одним из самых известных программных ассистентов на базе искусственного интеллекта и широко используется разработчиками для написания кода на различных языках. В приложениях для обеспечения кибербезопасности GitHub Copilot помог разработчикам создавать безопасные системы аутентификации, предлагая стандартные отраслевые методы обеспечения безопасности, такие

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

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

Аннотация