

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. «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

тәсіл қажет: заманауи технологияларды және қауіпсіздік шараларын үздіксіз жетілдіру, сондай-ақ техникалық және ұйымдастырушылық шараларды үйлестіру ақпараттық инфрақұрылымды тиімді әрі сенімді қамтамасыз етеді.

Қолданылған әдебиеттер

1. Microsoft Azure Security Essentials. 2021. URL: <https://learn.microsoft.com/en-us/azure/security/fundamentals/overview>
2. «Как вести бизнес через облачные сервисы.» URL: <https://secrets.tinkoff.ru/razvitie/oblachnye-servisy/>
3. Нестеренко В.Р., Маслова М.А. «Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними». Научный результат. Информационные технологии. – Т.6, №1, 2021. – С.48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6, URL: <http://rrinformation.ru/journal/annotation/2375/>
4. Миронова, А.О. «Применение методики оценки угроз безопасности информации». А.О. Миронова, Ю.Ю. Гончаренко, А.С. Гоголь, А.Н. Фролова // Энергетические установки и технологии. – 2021. – Т.7, №4, – С.71-75.
5. Облачные сервисы. URL: <https://corporatefinanceinstitute.com/resources/knowledge/data-analysis/cloud-services/>
6. Ожиганова, М.И. «Методы и средства проведения анализа угроз локальной вычислительной сети предприятия». М.И. Ожиганова, А.О. Шейко, Е.М. Исакова, А.О. Миронова // Цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021. – С.264-270.
7. Entra ID Diagram. URL: https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/Entra_ID_Diagram_new?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=3840&hei=1500&qtl=100&fit=constrain
8. Azure Sentinel End-to-End Security. URL: <https://gqadir.com/wp-content/uploads/2021/01/Azure-Sentinel-End-to-End-Security.png>
9. Azure Key Vault Overview Diagram. URL: https://learn.microsoft.com/en-us/azure/key-vault/media/key-vault-what-is/azurekeyvault_overview.png

ИОТ ҚҰРЫЛҒЫЛАРЫНЫҢ ЖЕЛІДЕГІ ҚАУІПСІЗДІГІН ҚАЛАЙ ҚАМТАМАСЫЗ ЕТУГЕ БОЛАДЫ: СТРАТЕГИЯЛАР ЖӘНЕ PACKET TRACER КӨМЕГІМЕН МОДЕЛЬДЕУ

Т. Сахатбекқызы., Т.А.Бахтиярқызы

tokaniasgtbk@gmail.com , arujan081204@gmail.com

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан.

Ғылыми жетекші: Казиева Назым Магидулловна

Аңдатпа

Мақалада IoT құрылғыларының элементтерінің желідегі қауіпсіздігін қамтамасыз ету мәселесі қарастырылған. IoT инфрақұрылымына төнетін негізгі киберқауіптер мен олардың әсері талданып, қорғаныс стратегиялары ұсынылды. Қауіпсіздік шаралары ретінде шифрлеу, аутентификация, желілік сегментация және жаңартулардың маңыздылығы сипатталады. Сонымен қатар, Cisco Packet Tracer ортасында IoT құрылғыларының қауіпсіздігін модельдеу әдістері сипатталған. Ұсынылған шешімдер IoT жүйелерін қорғаудың тиімділігін арттыруға бағытталған.

Кілт сөздер: IoT қауіпсіздігі, желілік шабуылдар, шифрлеу, аутентификация, Firewall, Packet Tracer, желілік модельдеу, киберқауіптер, мәліметтерді қорғау.

Кіріспе. XXI ғасыр цифрлық технологиялардың қарқынды дамыған дәуірі. IoT (Internet of Things) құрылғылары біздің күнделікті өміріміздің бір бөлігіне айналды. Ақылды үйлерден бастап өнеркәсіптік орындарға дейін IoT технологиялары процестерді автоматтандыруға және тиімділікті арттыруға көмектеседі. IoT құрылғылары қазіргі таңда шабуылдардың негізгі нысанына айналууда, өйткені олардың көпшілігі әлсіз қорғалған және желіге заңсыз қол жеткізуді жеңілдетеді.

Талқылаулар мен нәтижелер. IoT құрылғыларына төнетін қауіптер 2014 жылы Ресейде орын алған қызықты әрі үрей тудырлатын жағдай хакерлердің әрекеті, желіде ол «Шайнекпен келген шабуыл» атты атақты жағдайдан көруге болады. Мұнда хакерлер интернетке қосылған кәдімгі ақылды шайнектерді (смарт шайнек) пайдаланып, Wi-Fi осал желісін пайдалану арқылы, интернет провайдерлердің серверлеріне шабуыл жасады. Нәтижесінде адамзаттың қарапайым тұрмыста қолданып жатқан шайнектері хакерлік қаруға айналды!

IoT құрылғылары үлкен көлемде деректер жинайды, оның ішінде пайдаланушының жеке ақпараты, денсаулық көрсеткіштері, геолокациясы және күнделікті әдеттері болуы мүмкін. Бұл ақпарат хакерлердің қолына түссе, оны алаяқтық, бопсалау немесе басқа қылмыстық әрекеттер үшін қолдануы мүмкін. IoT тек тұрмыстық техникада ғана емес, өнеркәсіптік процестерде, денсаулық сақтау саласында және көлік жүйелерінде де жиі қолданылады. 2015 жылы Украинадағы энергетикалық инфрақұрылымға кибершабуыл жасалып, нәтижесінде бірнеше аймақтарда электр жарығы өшкендігін айтуға болады. Бұл шабуыл зиянды бағдарлама SCADA жүйелерін зақымдап, операторларға электр желілерін басқаруға мүмкіндік бермеді.

IoT құрылғыларының осалдықтарын жүйелі түрде қарастыру үшін негізгі қауіптер, олардың маңызы және Packet Tracer көмегімен модельдеу әдістері 1 кестеде сипатталған [1].

Кесте 1. IoT желі архитектурасының қауіпсіздік талдауы және қорғаныс стратегиялары

IoT желі элементі	Негізгі осалдықтар	Төнетін қауіптер	Жүйедегі рөлі мен ықпалы	Packet Tracer көмегімен қорғау және модельдеу әдісі
Датчиктер (физикалық құрылғылар)	Әлсіз шифрлау, аутентификацияның жоқтығы	Деректерді ұстап қалу, жалған ақпарат енгізу	Деректерді бастапқы жинау көзі, сенсорлық ақпараттың дұрыстығын қамтамасыз етеді	Қауіпсіздік хаттамаларын (TLS, WPA2) қолдану, құрылғылардың қауіпсіздігін тестілеу
Басқару блоктары (IoT-шлюздер)	Фирмалық протоколдарға тәуелділік, әлсіз брандмауэр	Желілік шабуылдар, құрылғыларды басқаруды қолға алу	IoT құрылғыларының арасындағы деректерді үйлестіру және өңдеу орталығы	Брандмауэрді күшейту, IDS/IPS қолдану, виртуалды модельдеу

Желі инфрақұрылымы	Әлсіз Wi-Fi қауіпсіздігі, ашық порттар	MITM (Man-in-the-Middle) шабуылы, рұқсатсыз қол жеткізу	Құрылғылар арасындағы ақпарат алмасудың негізгі арнасы	VLAN сегментациясы, VPN пайдалану, Packet Tracer-де қауіптерді модельдеу
--------------------	--	---	--	--

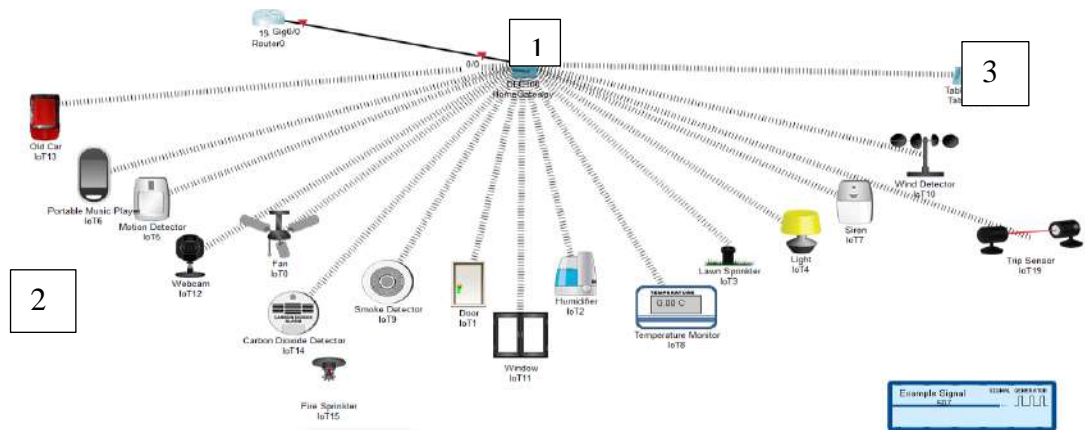
Packet Tracer көмегімен модельдеу

VLAN (Виртуалды жергілікті желі) бұл IoT құрылғыларын жеке желілерге бөлу.

VPN-интернеттегі деректерді шифрлайды және IP мекен жайын жасырады, осылайша қауіпсіз байланыс орнатады. 2018 жылы **Hapleton Bank** қаржы ұйымы қашықтан жұмыс істейтін қызметкерлерінің деректерін қорғау үшін **VPN қолданбаған**. Нәтижесінде, бір қызметкер **қоғамдық Wi-Fi желісіне** қосылып, шабуылдаушылар **банк жүйесіне рұқсатсыз кіріп**, клиенттердің **құпия қаржылық мәліметтерін ұрлаған**.

Packet Tracer-де ақылды үй (Smart home) IoT моделін жасау және қауіпсіздік баптаулары.

Бұл **Packet Tracer**-де модельденген **ақылды үй (Smart home) IoT желісінің топологиясы**. Сценарийде **бір Wi-Fi желісіне** қосылған әртүрлі **IoT құрылғылары** бар және олар **орталық шлюз (Home Gateway) арқылы** бақыланады.



Сурет 1. Packet Tracer –де IoT құрылғыларын модельдеу топологиясы

1. Home Gateway (DCE100) – барлық IoT құрылғыларын байланыстыратын негізгі басқару құрылғысы. Бұл шлюз IoT құрылғылары мен қолданушылар арасында деректер алмасуды басқарады. Желінің негізгі қауіпсіздігін қамтамасыз етеді.

2. IoT құрылғылары – әртүрлі смарт құрылғылар (терезе, есік, дабыл жүйелері, жарықтандыру, сенсорлар). Қауіпсіздік құрылғылары: қозғалыс детекторы (Motion Detector), веб-камера (Webcam), дабыл (Siren). Климаттық құрылғылар: температура датчигі (Temperature Monitor), ауа ылғалдандырғыш (Humidifier), жел сенсоры (Wind Detector). Үй автоматизациясы: желдеткіш (Fan), жарық шамы (Light), есік (Door), терезе (Window) Сурет 1.

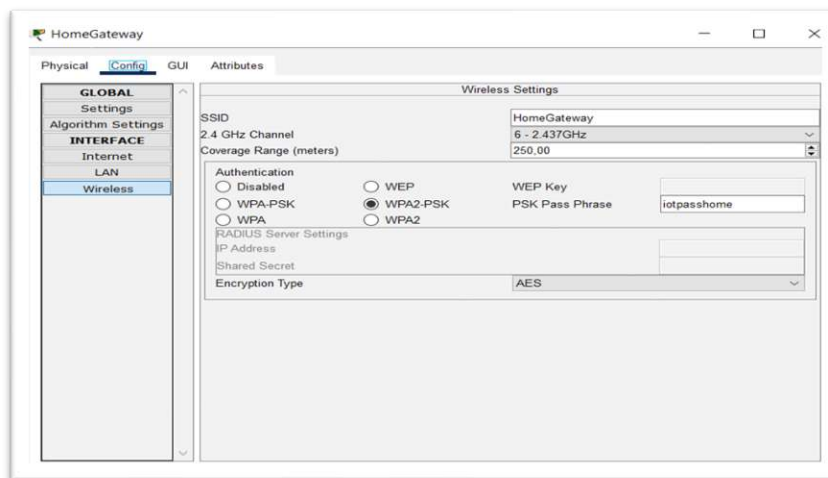
3 Планшет (Tablet PC) – IoT құрылғыларын қашықтан басқаруға және мониторинг жасауға мүмкіндік береді. Планшет Home Gateway-ге қосылып, арнайы интерфейс арқылы барлық құрылғылардың жұмысын көруге және басқаруға болады. Мысалы: қозғалыс сенсоры біреуді байқаса, планшетке хабарлама келеді. Суретте **Packet Tracer** ортасында әртүрлі IoT құрылғыларының планшетке қосылғанын көруге болады (сурет 2).



Сурет 2. IoT құрылғыларының қосылуы

IoT құрылғыларының осалдығы желідегі қорғалмаған құрылғылар арқылы хакерлердің бүкіл желіні бұзып кіруі.

IoT желісін құпия кілт орнату арқылы құрылғыларды ортақ желіге жалғап, «iotpasshome» паролін пайдаланып Home Gateway-ға қауіпсіз түрде қосылады. WPA2 - PSK аутентификациясы мен AES шифрлеуі деректердің қорғалуын қамтамасыз етеді, осылайша желідегі құрылғылардың қауіпсіздігі сақталады (сурет 3).



Сурет 3. WPA2-PSK аутентификациясы

Мысал ретінде құрылғылардың қозғалысына 2 команда бердім.

1 - команда. Қозғалыс анықталса ("person present"). Бұл шарт бойынша қозғалыс детекторы (IoT5) іске қосылғанда келесі әрекеттер орындалады:

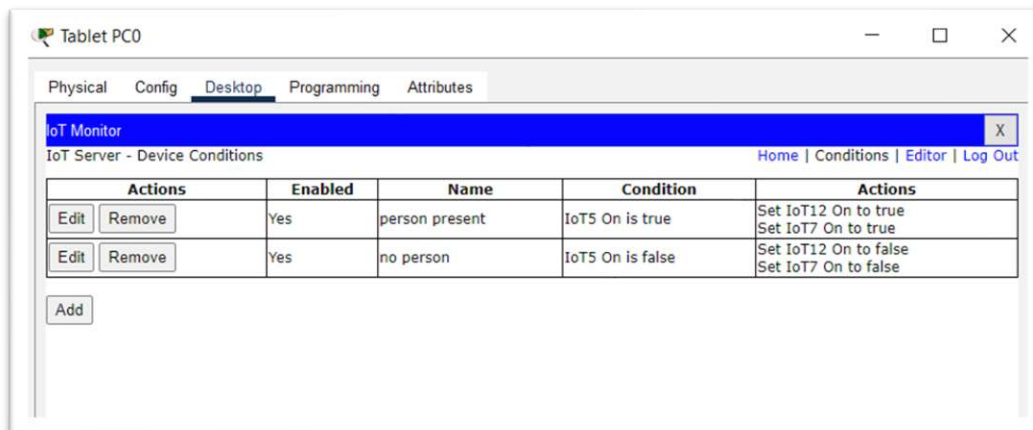
- ✓ Веб-камера (IoT12) жазба жүргізуді бастайды;
- ✓ Сирена (IoT7) дыбыс шығарады.

Бұл механизм бөлмеге адам кірген кезде қауіпсіздік шараларын автоматты түрде іске қосады.

2 – команда. Қозғалыс анықталмаса ("no person") егер қозғалыс детекторы (IoT5) ешқандай қозғалыс тіркемесе, онда келесі әрекеттер орындалады:

- ✓ Веб-камера (IoT12) өшіріледі.
- ✓ Сирена (IoT7) дабыл беруді тоқтатады.

Бұл шарт қажетсіз құрылғылардың жұмысын шектеу арқылы энергияны үнемдеуге және жүйенің тиімділігін арттыруға бағытталған. Осылайша, аталған екі команда арқылы қауіпсіздік жүйесі автоматтандырылып, қажетсіз қуат тұтыну азайтылады (сурет 4).

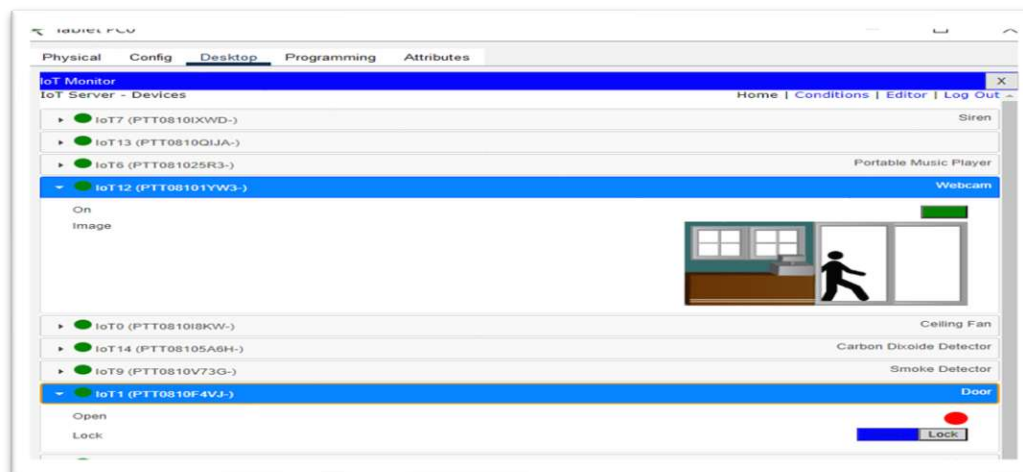


Сурет 4. Ереже орнату

Енді осы конфигурацияны тексеру барысында **Alt** батырмасын басып, қозғалыс детекторын (IoT5) іске қостым. Нәтижесінде:

- ✓ Сирена (IoT7) автоматты түрде іске қосылды.
- ✓ Веб-камера (IoT12) адам кіргені туралы белгі жіберді.

Бұл жүйе офлайн режимде қауіпсіздікті бақылауға мүмкіндік береді. Яғни, интернетсіз ақ детектор, сирена және камера өзара әрекеттесіп, қауіпсіздік шараларын автоматты түрде іске асырады (сурет 5).



Сурет 5. Қауіпсіздік жүйесін тексеру

Көрсетілген мысалдардан IoT құрылғылары арқылы қауіпсіздікті бақылауға болатынын көрдік. Бірақ мұндай жүйенің тұрақты әрі қауіпсіз жұмыс істеуі үшін арнайы желілік конфигурацияларды орындау керек. Төменде осыған қажетті негізгі қадамдар берілген.

1. Құпия сөздерді орнату және SSH конфигурациялау құрылғылардың қауіпсіздік арттыру үшін мықты құпия сөздер орнатылады және SSH қосылады > service password-encryption. Барлық құпия сөздерді шифрлау > crypto key generate rsa modulus 2048 – RSA кілтін генерациялау > transport input ssh Telnet-ті өшіріп, тек SSH қолдану.

2. VLAN құру және IoT құрылғыларын бөлу IoT құрылғылары үшін жеке VLAN орнату арқылы қауіпсіздік күшейтіледі > vlan 10. Жаңа VLAN құру > name IoT Devices – VLAN атауын беру > interface Gigabit Ethernet 0/1. Интерфейсті таңдау > switchport mode access. Портты қолжетімді режимге қою > switchport access vlan 10. Портты VLAN 10-ға қосу.

3. VPN (Virtual Private Network) конфигурациясы VPN IoT құрылғылары мен пайдаланушылар арасындағы қауіпсіз байланысты қамтамасыз етеді > crypto isakmp key VPNKey123 address 0.0.0.0 VPN кілтін орнату > crypto ipsec transform-set. MYSET esp-aes 256 esp-sha-hmac. Шифрлау параметрлерін орнату > crypto map VPNMAP 10 ipsec-isakmp – VPN картасын құру > set peer <Remote_IP> Қашықтағы құрылғыны анықтау > set transform-set MYSET. Шифрлау параметрлерін тағайындау > interface Gigabit Ethernet 0/0. VPN картасын интерфейске тағайындау > crypto map VPNMAP. VPN картасын қосу.

4. ACL (Access Control List) құру IoT құрылғыларына сыртқы қолжетімділікті шектеу үшін ACL пайдаланылады > access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22 – SSH арқылы рұқсат беру > access-list 100 deny ip any any – Басқа барлық трафикке тыйым салу > interface GigabitEthernet0/0 – Интерфейсті таңдау > ip access-group 100 in – ACL-ді кіріс трафигіне қолдану.

5. AAA (Authentication, Authorization, and Accounting) орнату IoT_Router жүйесіне кіруді басқару үшін AAA конфигурациясы орындалады > aaa authentication login default local – Аутентификацияны қосу > aaa authorization exec default local – авторизацияны қосу > aaa accounting exec default start-stop group tacacs+ – Бақылауды орнату.

6. NAT (Network Address Translation) конфигурациясы IoT құрылғыларының сыртқы желіге қауіпсіз қосылуын қамтамасыз ету үшін NAT қолданылады > ip nat inside source list 1 interface GigabitEthernet0/0 overload – NAT қызметін қосу.

Осы шаралар IoT құрылғыларының қауіпсіздігін күшейтіп, желіге рұқсатсыз қолжетімділіктің алдын алады

Қорытынды. IoT технологиясының қарқынды дамуы 2025 жылға қарай нарық көлемін 53,8 миллиард долларға дейін арттырады. Бұл өсім өнеркәсіптік автоматтандыруға сұраныстың ұлғаюымен байланысты. Алайда, IoT құрылғыларының қауіпсіздігі маңызды мәселе болып қалады, өйткені олардың 98% шифрланбаған трафикті пайдаланады, бұл кибершабуылдар мен деректер ұрлығын арттырады. Осы қауіптерді болдырмау үшін сенімді киберқауіпсіздік стратегиялары қажет. Желілік тренажерлер, мысалы, Packet Tracer, қауіпсіздік механизмдерін сынап, оңтайландыруда тиімді құрал бола алады. Шифрлау технологияларын енгізу, қауіпсіздік хаттамаларын жетілдіру және экожүйені қорғау тұрақты мониторингпен қамтамасыз етілуі тиіс.

Қолданылған әдебиеттер тізімі:

1. **Packet Tracer - Adding IoT devices to Smart Homes** - Cisco Networking Academy
2. **Introduction to the Internet of Things - Cisco Networking Academy**
3. Bruce Sinclair. IoT Inc: How Your Company Can Use the Internet of Things to Win in the Outcome Economy. 2017. 304 p.
4. Gurutech Networking Training. *Introduction to IoT Connecting & Simulating IoT Devices in Packet Tracer IoT Registration Server*. Қолжетімді: <https://youtu.be/qbh7SzCfM1o?si=yK3R25fwXpcw1fyi>
5. Techno Branch. *Smart Security System using Packet Tracer | IoT application | Anti Theft system using Packet Tracer*. Қолжетімді: <https://youtu.be/42DCkx36Uv8?si=Fkrbiq5FO8xTRk8a>
6. Analyzing Docker Vulnerabilities through Static Analysis.
7. Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review

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