

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

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

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

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

ISBN 978-601-08-5373-7

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

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

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

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

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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

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

Подсекция 2.2

Интеллектуальные информационные системы

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

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

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

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
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.	Мағзұмов 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

Бұл зерттеу аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерін құру үшін қолдану мүмкіндіктерін талдауға бағытталған. Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, K-Means және DBSCAN әдістерінің тиімділігі салыстырылды. Нәтижелер бойынша, ең тиімді аномалияларды анықтау құралдары ретінде Isolation Forest және LOF әдістері таңдалды. Бұл әдістер шынайы аномалияларды дәл және тұрақты түрде анықтап, ақпараттық қауіпсіздік жүйелерінің сенімділігін арттырады.

Ал K-Means әдісі аномалияларды анықтауда шамадан тыс сезімталдық танытып, жалған позитивтердің көптігіне әкелуі мүмкін, бұл оның ақпараттық қауіпсіздік жүйелерінде қолданылуын шектейді. DBSCAN және One-Class SVM әдістері де кейбір жағдайларда тиімді болуы мүмкін, бірақ олардың тұрақтылығы мен өнімділігі ақпараттық қауіпсіздік талаптарына толық сәйкес келе бермейді.

Зерттеу нәтижелері аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерінде қолдану үшін маңызды нұсқаулықтар ұсынады. Isolation Forest және LOF әдістері жоғары дәлдік пен тұрақтылықпен аномалияларды анықтауға мүмкіндік береді, сондықтан олар ИБ жүйелерінде кеңінен қолдануға тиімді болып табылады. Болашақ зерттеулерде осы әдістерді жетілдіру мен әртүрлі жағдайларда сынақтан өткізу арқылы олардың тиімділігін одан әрі арттыруға болады.

Қолданылған әдебиеттер тізімі

1. Xu H. et al. Deep isolation forest for anomaly detection //IEEE Transactions on Knowledge and Data Engineering. – 2023. – Т. 35. – №. 12. – С. 12591-12604.
2. Попова И. А. Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя Isolation Forest и Local Outlier Factor //StudNet. – 2020. – Т. 3. – №. 12. – С. 1460-1470.
3. Nuriddinovich K. S. Исследование обнаружения аномалий в сетевом трафике с использованием one-class svm //Journal of Modern Educational Achievements. – 2024. – Т. 1. – №. 1. – С. 214-222.
4. Ahmed M., Seraj R., Islam S. M. S. The k-means algorithm: A comprehensive survey and performance evaluation //Electronics. – 2020. – Т. 9. – №. 8. – С. 1295.
5. Deng D. DBSCAN clustering algorithm based on density //2020 7th international forum on electrical engineering and automation (IFEEA). – IEEE, 2020. – С. 949-953.
6. Котенко И. В. и др. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения //Информатика и автоматизация. – 2022. – Т. 21. – №. 6. – С. 1328-1358.

ӘӨЖ 004.056.5

КОРПОРАТИВТІК ЖЕЛІЛЕРДІ МОДЕЛЬДЕУ ЖӘНЕ ҚОРҒАУ

Бердибаев Көркем Сағындықұлы, Иманали Абылай Жандосұлы

b.korkem2004@gmail.com, imanali_05@mail.ru

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Бүгінгі цифрлық әлемде бизнес ақпараттық технологияларға толық тәуелді болғандықтан, корпоративтік желіні қорғау бірінші кезектегі маңызды міндетке айналады. Компаниялар күн сайын қарапайым вирустық шабуылдардан бастап, киберкылмыскерлердің

күрделі, үйлестірілген әрекеттеріне дейін көптеген қауіптерге тап болады. Мұндай жағдайда, деректердің ағып кетуі немесе желінің жұмысындағы іркіліс үлкен қаржылық шығындарға және беделге нұқсан келтіруге әкелуі мүмкін болғанда, корпоративтік желіні модельдеу және тиімді қорғау дағдылары ақпараттық қауіпсіздік саласындағы кез келген маман үшін өте маңызды.[3]

Бұл мақаланың мақсаты корпоративтік желілерді қорғаудың теориялық негіздеріне шолу жасау ғана емес, сонымен қатар желілерді модельдеуге арналған заманауи бағдарламалық құралдарды пайдалана отырып іске асырылуы мүмкін практикалық әдістерді көрсету болып табылады. Бұл құралдар шынайы желілердің модельдерін жасауға және бақыланатын ортада қорғаудың әртүрлі әдістерімен тәжірибе жасауға мүмкіндік береді, бұл оларды оқыту және дағдыларды жетілдіру үшін таптырмас құралға айналдырады.[4]

Біз желі инфрақұрылымын қалай дұрыс модельдеу керектігін, қандай негізгі қауіптер бар және оларды қалай болдырмауға болатынын қарастырамыз. Желілерді модельдеуге арналған танымал бағдарламалық құралдарды пайдалана отырып, межжелілік экрандарды баптаудың практикалық мысалдарына ерекше назар аударылады. Қадамдық нұсқаулар мен көрнекі мысалдар арқылы сіз теориялық концепциялардың нақты қауіпсіздік шараларына қалай айналатынын көре аласыз.

Бұл мақала студенттер мен ақпараттық қауіпсіздік саласындағы жаңадан бастаған мамандар үшін пайдалы нұсқаулық болуға бағытталған, оларға корпоративтік желілерді қорғаудың негіздерін түсінуге ғана емес, сонымен қатар осы қарқынды дамып келе жатқан салада жұмыс істеу үшін қажетті практикалық дағдыларды алуға көмектеседі.

Корпоративтік желіні модельдеу — нақты желілік инфрақұрылымның абстрактілі бейнесін жасау процесі. Ол желіні физикалық түрде орналастыруға дейін талдауға, жобалауға және оңтайландыруға мүмкіндік береді. Модельдеу желінің әртүрлі жағдайлардағы мінез-құлқын түсінуге, оның өнімділігін бағалауға және ықтимал осалдықтарды анықтауға көмектеседі.[5]

Негізгі принциптер:

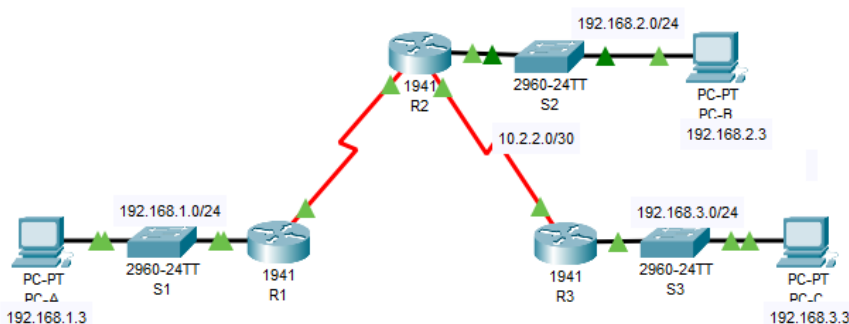
- **Логикалық топология:**
 - Деректердің желі арқылы қалай берілетінін сипаттайды.
 - IP-мекенжайын, VLAN, маршруттауды анықтайды.
 - Мысал: Бөлімдер мен серверлік аймақтарға бөлінген кәсіпорын желісінің құрылымы.

1 кесте. Логикалық топология.

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

- **Физикалық топология:**
 - Құрылғылардың және қосылымдардың физикалық орналасуын сипаттайды.
 - Кабельдердің, коммутаторлардың, маршрутизаторлардың түрлерін қамтиды.

■ Мысал: Сервер бөлмесіндегі желілік жабдықтың орналасуы және оны қосу тәсілі.



1 сурет. Физикалық топология.

○ Желілерді модельдеуге арналған бағдарламадағы қарапайым топологияның мысалы:

■ Бұл суретте біз желідегі негізгі байланыстарды түсіну үшін бірнеше компьютер, бір коммутатор және маршрутизатор сияқты желінің негізгі құрылымын орналастырамыз.

Негізгі қауіптер:

○ Сыртқы қауіптер:

■ Хакерлік шабуылдар: Желіге рұқсатсыз кіру.

■ Вирустар мен зиянды бағдарламалық қамтамасыз ету: Жүйеге зиян келтіретін

бағдарламалар.

○ Ішкі қауіптер:

■ Конфигурация қателері: Желілік жабдықты дұрыс баптамау.

■ Теріс пайдалану: Қызметкерлердің заңсыз әрекеттері.

○ Шабуылдардың негізгі түрлері:

■ DoS/DDoS шабуылдары: Желіні трафикпен шамадан тыс жүктеу.

■ Фишинг: Алдау арқылы деректерді ұрлау.

Қорғаудың негізгі құралдарына кіріспе:

○ Желіаралық экрандар (firewalls):

■ Кіріс және шығыс трафигін бақылайды.

■ Ережелер негізінде трафикті сүзгілейді.

○ Шабуылдарды анықтау жүйелері (IDS):

■ Күдікті әрекеттердің бар-жоғын трафикті талдайды.

■ Ықтимал шабуылдар туралы ескертеді.

○ Қол жеткізуді бақылау (ACL):

■ Қол жеткізуді бақылау тізімдері маршрутизатор немесе коммутатор интерфейсі арқылы қандай трафиктің өтуі мүмкін екенін анықтайды.

■ IP-мекенжайлары, порттар және хаттамалар негізінде трафикті сүзу үшін пайдаланылады.

Біз модельдеуге арналған бағдарламалық қамтамасыз ету мүмкіндіктерін пайдалана отырып, корпоративтік желілерді қорғаудың теориялық білімдерін практикалық қолдануға тереңірек кіреміз. Негізгі назар межжелілік экрандар, шабуылдарды анықтау жүйелері және виртуалды жеке желілер сияқты қауіпсіздіктің негізгі құралдарын баптау мен жұмысын көрсетуге аударылады.

Желілік қауіпсіздікте іргелі рөл атқаратын межжелілік экрандардан бастайық, олар трафикті бақылайды және берілген ережелер негізінде сүзеді. Олардың түрлері әртүрлі болуы

мүмкін: қарапайым пакеттік сүзгілерден бастап күрделі күйді қадағалайтын межжелілік экрандарға және веб-қосымшаларды қорғауға арналған мамандандырылған WAF-тарға дейін.

Біз трафикті басқару үшін кеңейтілген ACL-ді қалай баптау керектігін, қандай пакеттерге рұқсат етіліп, қандай пакеттерге тыйым салынғанын анықтайтынын көрсетеміз.[1]

```
enable
configure terminal

access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any

interface FastEthernet0/0
ip access-group 1 out

access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 101 permit ip any any

interface FastEthernet0/1
ip access-group 101 in

show access-lists

no access-list 1
no access-list 101
```

3 сурет. ACL-мен желілік трафикті филтьрлеу.

Содан кейін біз желідегі аномалиялар мен күдікті әрекеттерді анықтай отырып, қауіптерді бақылауға қызмет ететін шабуылдарды анықтау жүйелеріне көшеміз. IDS-нің желілік және хосттық жүйелерді қоса алғанда, әртүрлі түрлері бар. Біз порттарды сканерлеу немесе DoS шабуылдары сияқты нақты шабуыл түрлерін анықтау үшін негізгі IDS-ді қалай баптау керектігін көрсетеміз және оқиғалардың үрдістері мен оқиғаларын анықтау үшін IDS журналдарын қалай талдау керектігін көрсетеміз.[2]

Желінің үздіксіз жұмыс істеуін қамтамасыз ету үшін резервтік арналардың болуы және циклдардың алдын алу үшін STP сияқты хаттамаларды қолдану маңызды. Біз STP бар сақиналық топологияны қалай құруға болатынын және желі қауіпсіздігін күшейту үшін Cisco IOS командаларын қалай пайдалануға болатынын көрсетеміз.

Корпоративтік желіні модельдеу желіні нақты орналастыруға дейін талдауға, жобалауға және оңтайландыруға мүмкіндік беретін маңызды кезең болып табылады. Бұл тек ықтимал осалдықтарды анықтауға ғана емес, сонымен қатар желі жұмысының тиімділігін айтарлықтай арттыруға мүмкіндік береді. Межжелілік экрандар алдыңғы қатарлы қорғаныс болып табылады, трафикті бақылайды және рұқсатсыз кіруге жол бермейді, ал шабуылдарды анықтау жүйелері желіні үнемі бақылап, күдікті әрекеттерді анықтап, ескертеді. Резервтік арналар көмегімен ақауларға төзімді желілерді құру жұмыстың үздіксіздігін және қауіпсіз қашықтағы қол жеткізуді қамтамасыз етеді.

Корпоративтік желіні қорғау үздіксіз процесс екенін атап өту қажет. Бағдарламалық жасақтама мен дерекқорларды үнемі жаңарту, сондай-ақ желілік трафикті тұрақты бақылау талап етіледі. Бұлтты есептеу және заттар интернеті сияқты технологиялардың қарқынды дамуын ескере отырып, ақпараттық қауіпсіздік саласындағы соңғы үрдістерден хабардар болу маңызды.

Желілерді модельдеу арқылы білімді практикалық қолдану ақпараттық қауіпсіздік бойынша білікті мамандарды даярлаудың ажырамас бөлігі болып табылады. Желілерді модельдеуге арналған бағдарламалармен жұмыс істеу барысында алынған дағдылар қауіпсіз желі ортасын құру және қолдау арқылы теориялық білімді практикада тиімді қолдануға мүмкіндік береді.

Қолданылған әдебиеттер тізімі

1. Configure Commonly Used IP ACLs - Cisco Documentation
2. Современные проблемы безопасности корпоративных сетей - Н. Андреев
3. "Безопасность корпоративных сетей / Учебно-методическое пособие" - Биячуев Т.А., Осовецкого Л.Г.
4. "Построение защищенных корпоративных сетей" - Рашид Ачилов
5. "Практическая безопасность сетей" - NetSkills

УДК 004.056.5

АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ С ПОМОЩЬЮ ИИ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Ерболатов Али

alierbolatov9@gmail.com

Магистрант кафедры Информационной безопасности, Астана, Казахстан
Научный руководитель – Сантеева Сая Әділбайқызы, PhD, старший преподаватель

Аннотация: Статья посвящена анализу использования искусственного интеллекта (ИИ) для выявления и анализа вредоносных программ, а также рассмотрению криптографических методов защиты от таких угроз. С развитием технологий ИИ возрастает угроза их использования для создания вредоносных программ, что делает необходимым разработку эффективных механизмов защиты. В статье рассматриваются основные методы защиты ИИ, включая шифрование, обфускацию и дифференциальную приватность, а также способы их применения в контексте защиты от реверс-инжиниринга и атак. Особое внимание уделено интеграции ИИ и криптографических технологий для создания более безопасных и устойчивых к угрозам систем. Исследуются примеры реальных атак на модели ИИ и способы их предотвращения с использованием современных технологий защиты. Предложены рекомендации по усилению безопасности ИИ-моделей и перспективы развития в этой области.

Ключевые слова: искусственный интеллект, криптография, защита данных, вредоносные программы, реверс-инжиниринг, шифрование, обфускация, дифференциальная приватность, киберугрозы, атаки на данные, машинное обучение, безопасность ИИ.

Введение

С развитием технологий искусственного интеллекта (ИИ) в последние десятилетия они начинают играть ключевую роль в различных областях, таких как медицина, финансы, кибербезопасность и многие другие. Однако с увеличением применения ИИ возрастает и угроза его использования в злонамеренных целях, таких как создание вредоносных программ. Вредоносные программы, использующие ИИ, могут эффективно обходить традиционные методы защиты, что требует разработки более инновационных и гибких защитных систем [1, с. 18].

Одной из основных проблем, с которой сталкиваются специалисты по безопасности, является реверс-инжиниринг моделей ИИ. Этот процесс позволяет злоумышленникам извлекать информацию о внутренней структуре и параметрах модели, что открывает возможности для атак на данные или кражи интеллектуальной собственности. Для защиты ИИ от таких угроз активно разрабатываются различные методы, включая шифрование, обфускацию нейросетевых весов и использование дифференциальной приватности [2, с. 45].

Целью данной работы является анализ применения искусственного интеллекта для