

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

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

ISBN 978-601-08-5373-7

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

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

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

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

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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

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

Подсекция 2.2

Интеллектуальные информационные системы

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

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

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

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

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

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Раматуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

ELF ТАЛДАУЫНДАҒЫ CAPSTONE: СЫЗЫҚТЫҚ ЖӘНЕ РЕКУРСИВТІ ДИЗАССЕМБЛЕРЛЕУ

Кеттеш Бекнұр Нұрланұлы
kbeknurt@mail.ru

Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс
магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Ж.Сауханова

Дизассемблерлеу – екілік файлдарды талдаудың негіздерінің бірі. Дизассемблерлеу машина кодын неғұрлым түсінікті ассемблер көрінісіне түрлендіруге және бағдарламаның құрылымы мен логикасын тереңірек түсінуге мүмкіндік береді. Бағдарламалық кодты қорғау мен обфускациялаудың үнемі күрделене түсуіне байланысты мақалада ұсынылған әдістерді қолдану нәтижесінде талдаушы өзінің зерттеуінің дәлдігі мен тиімділігін едәуір арттыра алады.

Бинарлық файлдарды талдауда дизассемблердің стандартты болжамдары бұзылған жағдайда дизассемблердің арнайы өтуі қажет болады. Мысалы, зиянды бағдарламаны, обфускацияланған файлдарды, жады немесе бағдарламалық жасақтаманың дампытарын талдау барысында. Сонымен қатар, кодтағы осалдықтарға нұсқайтын үлгілерді іздеу барысында да дизассемблердің арнайы өтулері бинарлық талдаудың ерекше түрлерін оңай жүзеге асыруға мүмкіндік береді. Бұл сондай-ақ дизассемблирлеудің жаңашыл әдістерімен тәжірибе жасауға мүмкіндік беретін пайдалы зерттеу әдісі.

Арнайы дизассемблирлеудің алғашқы нақты мысалы ретінде командалардың қабаттасуы (overlapping instructions) арқылы код обфускациясын зерттеу қарастырылады. Көптеген дизассемблерлер әрбір бинарлық файл үшін тек бір листинг жасайды, өйткені олар әрбір байт тек бір ғана командаға қатысты екенін білдіреді, әрбір команда бір қарапайым блокқа тиесілі және әрбір қарапайым блок бір ғана функцияның бөлігі болып табылады деп болжайды. Басқаша айтқанда, дизассемблерлер кодтың бөліктері бір-бірімен қабаттаспайды деп есептейді. Алайда, командалардың қабаттасуы бұл болжамды бұзады, кері инженерияны қиындатады. Командалардың қабаттасуы x86 платформасында мүмкін, өйткені бұл платформада командалардың ұзындығы әртүрлі (ARM сияқты кейбір басқа платформалардан айырмашылығы, онда барлық командалар бірдей байт санынан тұрады). Сондықтан процессор командаларды жадыда арнайы туралауды талап етпейді, бұл бір команданың басқа команда алған мекенжайларды иеленуіне мүмкіндік береді. Осыған байланысты x86 жүйесінде дизассемблирлеуді команданың ортасынан бастап, алғашқы командамен ішінара немесе толықтай қабаттасатын басқа команданы алуға болады.

Capstone – бұл x86/x86-64, ARM, MIPS және басқа да ең танымал командалар архитектураларын өңдеуге мүмкіндік беретін қарапайым әрі жеңіл API ұсынатын дизассемблирлеу кітапханасы. Ол C/C++ және Python (сондай-ақ басқа да тілдер) интерфейстеріне ие. Кітапхана Windows, Linux және macOS сияқты барлық танымал платформаларда жұмыс істейді. Capstone мүлдем тегін және ашық бастапқы кодқа ие.

Capstone көмегімен дизассемблирлеу құралдарын жасау – өте икемді әрі қарапайым процесс. API негізінде бірнеше ғана функциялар мен деректер құрылымдары болғанымен, бұл оны қолданудың ыңғайлылығына еш әсер етпейді. Capstone дизассемблирленген командалар туралы маңызды мәліметтерді алуды айтарлықтай жеңілдетеді. Оларға операция кодтары, мнемоникалар, класс, команда пайдаланатын және өзгертін регистрлер мазмұндары және тағы басқа деректер жатады.

Зерттеу барысында дизассемблерлеу процестерін тереңірек талдауға мүмкіндік беретін Capstone кітапханасын қолдану арқылы екі түрлі әдіс қарастырылды. Бұл екі тәсіл – сызықтық дизассемблерлеу және рекурсивті дизассемблерлеу – бір қарағанда ұқсас болғанымен, олардың жұмыс істеу принциптері мен қолдану салалары айтарлықтай ерекшеленеді.

Алдымен сызықтық дизассемблерлеу мысалы қарастырылады.

Python көмегімен x86_64 платформасы үшін Сурет 1-де дизассемблерлеу сызықтық дизассемблерлеудің мысалы келтірілген:

```
# -*- coding: utf-8 -*-
from capstone import *

CODE = b"\x55\x48\x8b\x05\xb8\x13\x00\x00"

md = Cs(CS_ARCH_X86, CS_MODE_64)
for i in md.disasm(CODE, 0x1000):
    print("0x%x:\t%s\t%s" % (i.address, i.mnemonic, i.op_str))
```

Сурет 1. linear_disassembler.py файлы

Бұл код Capstone көмегімен бинарлық кодты x86_64 ассемблер тіліне аударады. Енді әр жолды егжей-тегжейлі қарастырайық.

1. Capstone кітапханасын импорттау

```
from capstone import *
```

Бұл жол Capstone кітапханасын жүктейді, осылайша оны Python кодымызда қолдана аламыз.

2. Бинарлық кодты анықтау

```
CODE = b"\x55\x48\x8b\x05\xb8\x13\x00\x00"
```

Бұл x86_64 платформасында орындалатын бинарлық код. Әрбір \x.. мәні – бұл машиналық кодтың бір байты.

3. Дизассемблер объектісін жасау

```
md = Cs(CS_ARCH_X86, CS_MODE_64)
```

Мұнда Capstone дизассемблер объектісін құрылады. Ол екі негізгі параметрді алады:

CS_ARCH_X86 – x86 архитектурасын көрсетеді

CS_MODE_64 – 64-биттік режимде жұмыс істеу керектігін білдіреді

4. Дизассемблирлеу процесі

```
for i in md.disasm(CODE, 0x1000):
```

```
    print("0x%x:\t%s\t%s" % (i.address, i.mnemonic, i.op_str))
```

Бұл цикл Capstone дизассемблерін CODE айнымалысына қолданады және оның нәтижесін экранға шығарады. 0x1000 – виртуалды мекенжай, яғни дизассемблерленген кодтың бастапқы орны ретінде қабылданатын мекенжай.

Әрбір нұсқау үш негізгі өріске бөлінеді:

i.address – команда орналасқан мекенжай

i.mnemonic – команданың ассемблерлік мнемоникасы

i.op_str – команданың операндтары

linear_disassembler.py файлын іске қосу нәтижесі Сурет 2-де көрсетілген.

```
binary@binary-VirtualBox:~$ python linear_disassembler.py
0x1000: push    rbp
0x1001: mov     rax, qword ptr [rip + 0x13b8]
```

Сурет 2. linear_disassembler.py кодының нәтижесі

Нәтиже төмендегідей болады:

```
0x1000: push rbp
```

```
0x1001: mov raх, qword ptr [rip + 0x13b8]
```

Бұл бинарлық кодты оқылатын ассемблер тіліне айналдырғанымызды білдіреді. Әр жолды жеке қарастырайық:

```
0x1000: push rbp
```

push rbp командасы стекке rbp регистрінің мәнін сақтайды.

Бұл функцияның прологы ретінде жиі қолданылады. Келесі жол:

```
0x1001: mov raх, qword ptr [rip + 0x13b8]
```

mov raх, qword ptr [rip + 0x13b8] – rip регистріндегі мәнге 0x13b8 санын қосып пайда болған мәнге сәйкес адреске орналасқан 8 байтты деректі raх регистріне жүктейді.

Мұндай операция динамикалық жүктелетін деректерді немесе жадыдағы мәндерді оқу үшін қолданылады.

Сызықтық дизассемблер кодты біртіндеп, рет-ретімен талдайды және оның ішінде қандай да бір тармақталу немесе секіру орын алса да, ол келесі команданы бірізді түрде оқи береді. Мұнда Capstone кітапханасының CS класын қолданылды, ол x86_64 архитектурасында 64-биттік кодты дизассемблерлеуге мүмкіндік береді. Алдымен машиналық код CODE айнымалысына бинарлық түрде енгізіліп, содан кейін ол md.disasm() функциясы арқылы талданды. Нәтижесінде дизассемблерленген кодтың түсінікті форматы алынғанын көруге болады. Дегенмен, бұл тәсілде кодтың орындалу бағыты өзгерсе немесе секіру командалары қолданылса, талдау толық болмай қалуы мүмкін. Сондықтан, күрделі бағдарламаларды зерттеу үшін рекурсивті дизассемблерлеу әдісін пайдалану қажет.

Рекурсивті дизассемблер кодтың орындалу бағытын ескере отырып, дизассемблерлеу жасайды. Сурет 3-те көрсетілген recursive_disasm() функциясы белгілі бір мекенжайдан бастап дизассемблерлеуді жүзеге асыратындай етіп құрылды. Бұл әдіс кодтың ішінде кездесетін jmp және call командаларын талдайды және олар сілтейтін жаңа мекенжайларды да дизассемблерлеу үшін queue тізіміне қосады. Осылайша, орындалу барысында шын мәнінде қандай командалар орындалатыны нақты анықталады.

```
# -*- coding: utf-8 -*-
from capstone import *

def recursive_disasm(code, start_addr):
    visited = set()
    queue = [start_addr]
    md = Cs(CS_ARCH_X86, CS_MODE_64)

    while queue:
        addr = queue.pop()
        if addr in visited:
            continue
        visited.add(addr)

        for i in md.disasm(code, addr):
            print("0x%x:\t%s\t%s" % (i.address, i.mnemonic, i.op_str))
            if i.mnemonic in ['jmp', 'call']:
                try:
                    queue.append(int(i.op_str, 16))
                except ValueError:
                    pass # Если переход не на конкретный адрес

CODE = b"\x55\x48\x8b\x05\xb8\x13\x00\x00\xff\xe0" # содержит "jmp raх"
recursive_disasm(CODE, 0x1000)
```

Сурет 3. recursive_disassembler_code файлы

Нәтижесінде, егер кодта jmp немесе call кездессе, рекурсивті дизассемблер олардың көрсеткен жаңа мекенжайларын да талдап, толық талдау жүргізеді. Тәжірибе көрсеткендей,

бұл әдіс сызықтық дизассемблерлеуге қарағанда анағұрлым тиімді және сенімді. Мысалы, jmp rax командасы орындалған кезде, келесі орындалатын команда жаңа мекенжайда болуы мүмкін, ал рекурсивті дизассемблер осы жағдайды ескереді. Обфускаторлар ешқашан пайдаланылмайтын жалған жолдарды құру арқылы көбінесе сызықтық дизассемблерлерді шатастыруға тырысады. Ол үшін әрдайым ақиқат немесе әрдайым жалған болатын предикаттар қолданылады, бірақ дизассемблер оларды тани алмайды. Мұндай қиын анықталатын предикаттар көбінесе сандық теңдіктерді немесе көрсеткіштерді біріктіру әдістерін қолдану арқылы жасалады.

Кодта кездесетін jmp командасының талдауы Сурет 4-те көрсетілген.

```
binary@binary-VirtualBox:~$ python recursive_disassembler.py
0x1000: push    rbp
0x1001: mov     rax, qword ptr [rip + 0x13b8]
0x1008: jmp    rax
```

Сурет 4. recursive_disassembler кодының нәтижесі

Нәліктен арнайы дизассемблер үзіндісін жазу керек?

IDA Pro, Ghidra, Radare2 сияқты стандартты дизассемблерлер кең мүмкіндіктерге ие, бірақ әрқашан кодты дұрыс түсіндіре бермейді. Проблемалар келесі жағдайларда пайда болады:

- Кодты бұзу. Кейбір екілік файлдарда артық нұсқаулар, өзін-өзі өзгертетін код бар, бұл талдауды қиындатады.
- Стандартты емес нұсқауларды пайдалану. Мысалы, Кеңейтілген командалар жиынтығы бар процессорларға (SSE, AVX) стандартты құралдар қолдау көрсетпеуі мүмкін.
- Код пен деректерді бөлу. Кейбір ELF бөлімдерінде дизассемблер орындалатын код ретінде қате түсіндіретін деректер болуы мүмкін.

Қорытынды

Зерттеу барысында Capstone кітапханасының көмегімен бинарлық кодты дизассемблерлеу әдістерінің екі түрі – сызықтық және рекурсивті тәсілдері талданды. Сызықтық дизассемблерлеу қарапайым, тікелей және жылдам болып табылады, алайда тармақталу және секірулер бар жағдайларда кейбір маңызды нұсқауларды жіберіп алуы мүмкін. Ал рекурсивті тәсіл орындалу логикасын толығырақ ескере отырып, кодтың барлық ықтимал орындалу жолдарын зерттеуге мүмкіндік береді, бұл күрделі бағдарламаларды талдауда аса маңызды.

Қорытындылай келе, әрбір әдістің өз артықшылықтары мен кемшіліктері бар екенін атап өткен жөн. Сызықтық тәсіл қарапайым және жылдам талдау жүргізуге мүмкіндік берсе, рекурсивті тәсіл кодтың нақты орындалу ағымын толық түсінуге септігін тигізеді. Capstone кітапханасының икемді API-і бұл екі әдісті де тиімді жүзеге асыруға мүмкіндік беріп, бинарлық файлдарды талдау, кері инженерия және қауіпсіздік зерттеулері салаларында қуатты құрал ретінде қолданылуын қамтамасыз етеді. Осылайша, зерттеушілер өздерінің нақты қажеттіліктеріне байланысты сәйкес әдісті таңдап, талдау процесін барынша тиімді жүргізе алады.

Қолданылған әдебиеттер тізімі

1. Эндрюс Д. Практический анализ двоичных файлов. – М.: Бином, 2022. – 223 с.
2. Эриксон Д. Hacking: The Art of Exploitation. – San Francisco: No Starch Press, 2004. – 480 с.

3. Данг Б., Газет А., Бачаалани Е., Жоссе С. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. – Indianapolis: Wiley, 2014. – 120 с.
4. Юричев Д. Reverse Engineering for Beginners. – М.: O’Reilly, 2011. – 350 с.
5. Эйлам Э. Reversing: Secrets of Reverse Engineering. – Indianapolis: Wiley, 2005. – 78 с.

УДК 004

LINUX ҚОРҒАУДЫҢ ЗАМАНАУИ ӘДІСТЕРІНЕ ТАЛДАУ.OPENVAS ЖӘНЕ NMAP КӨМЕГІМЕН ОСАЛДЫҚТАРДЫ АНЫҚТАУ.

Көшкінбаева Фариза Қонайқызы

fari_01-21@list.ru

Қ.Жұбанов атындағы Ақтөбе өңірлік университеті, магистрант, Ақтөбе, Қазақстан
Ғылыми жетекшісі – Г.А.Шангытбаева

Аннотация. Мақалада Openvas және Nmap құралдары арқылы осалдықтарды анықтауға ерекше назар аудара отырып, Linux операциялық жүйесін қорғаудың заманауи әдістері қарастырылады. Зерттеу желілік трафиктің осалдықтарын сканерлеу процесін, сондай-ақ Linux жүйелерінің қауіпсіздігі контекстінде осы құралдарды қолдану тиімділігін бағалауды сипаттайды. Талдау жүргізу үшін Kali Linux қолданылады — ең танымал қауіпсіздік тестілеу платформаларының бірі. Мақалада Openvas және Nmap жұмысының негізгі принциптері, олардың осалдықтарды анықтаудағы ерекшеліктері мен артықшылықтары, сондай-ақ инфрақұрылымның жалпы қауіпсіздігін жақсартуға ықпал ететін жүйелерді бақылау және шабуылдан қорғау процесіне біріктіру мүмкіндіктері егжей-тегжейлі қарастырылады.

Кілт сөздер: қауіпсіздік құралдары, OpenVAS, Nmap, осалдықтар, сканерлеу

Аннотация. В статье рассматриваются современные методы защиты операционной системы Linux, с особым акцентом на обнаружение уязвимостей с помощью инструментов OpenVAS и Nmap. В ходе исследования будет описан процесс сканирования уязвимостей сетевого трафика, а также оценка эффективности применения этих инструментов в контексте безопасности Linux-систем. Для проведения анализа используется Kali Linux — одна из самых популярных платформ для тестирования безопасности. В статье подробно рассмотрены основные принципы работы OpenVAS и Nmap, их особенности и преимущества в выявлении уязвимостей, а также возможности их интеграции в процесс мониторинга и защиты систем от атак, что способствует улучшению общей безопасности инфраструктуры.

Ключевые слова: инструменты безопасности, OpenVAS, Nmap, уязвимости, сканирование

Annotation. The article discusses modern methods of protecting the Linux operating system, with a special focus on vulnerability detection using OpenVAS and Nmap tools. The study will describe the process of scanning network traffic vulnerabilities, as well as evaluating the effectiveness of using these tools in the context of Linux system security. Kali Linux, one of the most popular security testing platforms, is used for the analysis. The article discusses in detail the basic principles of OpenVAS and Nmap, their features and advantages in identifying vulnerabilities, as well as the