ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM 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, докоранттардың 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 имолодыхученых 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 КОММ УНИКАЦИОННЫЕ 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.	Сагындыкова 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 курсын оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсында 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 Жасиинович «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 аі 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.	Аскаров 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 soar 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 инцитенттеріне 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.	Магзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсеитов 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 *geranium sanguineum* 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 морфофунционалдық 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

2. Positive research. Практикалық қауіпсіздік бойынша зерттеулер жинағы. [Электрондық ресурс]. Қол жеткізу режимі: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2017-rus.pdf/

3. Алдау өнері / Кевин Митник, Уильям Саймон. М.: ВМиК МГУ баспа бөлімі. МАКС Пресс баспасы, 2018.

4. Whitman, M. E., & Mattord, H. J. (2020). *Principles of Information Security* (6th ed.). Cengage Learning.

5. Symantec Corporation**. (2020). *2019 Internet Security Threat Report*. Symantec.

- A detailed annual report that highlights trends in cybersecurity threats, including social engineering. It provides real-world case studies and advice on securing employees from these types of attacks. [Link: https://www.broadcom.com/company/newsroom/press-releases?filtr=internet-security-threat-report]

УДК: 004.056.5

WEBSOCKET ПРОТОКОЛЫНДАҒЫ ОСАЛДЫҚТАРДЫ ТАЛДАУ

Магзумов Алихан Маратұлы
alihan.magzumov@mail.ru
Л.Н.Гумилев атындағы ақпараттық қауіпсіздік факультетінің магистрантты
Ғылыми жетекші – Ж.Сауханова

Аннотация: Бұл мақалада WebSocket протоколының осалдықтарын зерттеу және талдау әдістері қарастырылады. Нақты шабуыл мысалдары негізінде WebSocket байланыстарының қауіпсіздік мәселелері талданып, олардың ақпараттық жүйелерге ықтимал әсері бағаланады. Сондай-ақ осалдықтарды пайдаланудың негізгі әдістері мен оларды анықтау жолдары көрсетіледі. WebSocket байланыстарын қорғау және шабуылдардың алдын алу бойынша ұсыныстар беріледі. Мақала ақпараттық қауіпсіздік саласындағы мамандарға, зерттеушілерге және веб-қосымшалар әзірлеушілеріне арналған.

Кілт сөздер: Веб-қосымша, Интернет-ресурс, Websocket, қауіпсіздік, осалдық, ақпарат жинау.

Ақпараттық қауіпсіздіктегі осалдық - шабуылдаушылар қолдана алатын ақпараттық активтің немесе бақылау мен басқарудың әлсіз жақтары. Ақпараттық қауіпсіздіктің осалдықтарының жіктелуі өте көп. Соның ішінде веб-қосымшалардағы Websocket осалдықты ескерген жөн. Өйткені бұл қосымшаның және онымен байланысты деректердің құпиялылығына, тұтастығына және қол жетімділігіне нұқсан келтіруі мүмкін қауіпсіздік қатерлері мен шабуылдарына жол береді.

WebSocket осалдықтарын және олардың веб-қосымшалар үшін салдарын зерттеу әдістемесі теориялық талдауды және қауіпсіздік әдістерін әзірлеуді біріктіретін кешенді тәсілді қамтиды.

WebSocket – бұл екі жақты нақты уақыттағы деректер алмасуды қамтамасыз ететін хаттама. Ол веб-қосымшалардағы жылдамдық пен тиімділікті арттырады, бірақ сонымен бірге жаңа қауіпсіздік қатерлерін де тудырады. WebSocket хаттамасының ерекшелігі – тұрақты қосылым орнату арқылы сервер мен клиент арасында үздіксіз байланыс жасауында. Бұл механизм дәстүрлі HTTP сұраныс-жауап үлгісінен ерекшеленеді және дұрыс қорғалмаған жағдайда осалдықтарға жол ашады.

WebSocket тиімділік, масштабталу және икемділік тұрғысынан көптеген артықшылықтар ұсынады, бірақ сонымен қатар шабуылдаушылар пайдалана алатын бірқатар осалдықтарды да қамтиды. Ең көп таралған WebSocket осалдықтар мыналар:

1. Аутентификация мен авторизацияның болмауы – жүйенің пайдаланушыны танымайтын (аутентификация) немесе оның рұқсаттарын тексермейтін (авторизация) осалдығы. Бұл шабуылдаушыларға деректер мен жүйенің мүмкіндіктеріне рұқсатсыз қол жеткізуге мүмкіндік береді.

Мысал: Егер WebSocket сессиясы бір рет орнатылғаннан кейін қайта аутентификация талап етпесе, шабуылдаушы қолданыстағы сессияны ұстап алып, жәбірленуші атынан команда жіберуі мүмкін.

2. Деректерді ашық түрде беру - деректер шифрланбай, үшінші жақтың оңай ұстап алып, өзгерте алу мүмкіндігі. Бұл құпия деректердің, соның ішінде пайдаланушы тіркелгілерінің және төлем ақпаратының ұрлануына әкелуі мүмкін

Мысал: ws:// орнына wss:// қолданбаса, WebSocket арқылы жіберілетін деректер желіде ашық беріледі, бұл шабуылдаушыларға оларды ұстап алуға мүмкіндік береді.

3. SQL-инъекция немесе командалық инъекция - шабуылдаушы зиянды кодты дерекқор сұраныстарына немесе жүйенің командалық интерфейсіне енгізетін осалдық. Бұл деректерді оқу, өзгерту, жою немесе серверде еркін командалар орындауға мүмкіндік береді.

Мысал: Егер сервер WebSocket хабарламаларын дұрыс тексермесе, шабуылдаушы SQL немесе жүйелік командаларды орындау арқылы деректерге рұқсатсыз қол жеткізе алады.

4. XSS (Кросс-сайттық сценарий шабуылы) - пайдаланушының браузерінде зиянды сценарийлерді орындауға мүмкіндік беретін осалдық. Бұл сессия деректерін ұрлауға, веб-бет мазмұнын өзгертуге немесе пайдаланушы атынан зиянды әрекеттер жасауға әкелуі мүмкін.

Мысал: Егер WebSocket-тен алынған деректер браузерде сүзгіленбей көрсетілсе, шабуылдаушы зиянды JavaScript енгізіп, құрбанның сессиясын ұрлауы мүмкін.

5. JSON Web Token (JWT) немесе сессия токендері арқылы шабуыл - токендерді бұзу, ұрлау немесе өзгерту арқылы пайдаланушы атынан заңсыз әрекеттер жасау осалдығы. Бұл қорғалған ресурстарға рұқсатсыз қол жеткізуге немесе басқа пайдаланушылардың құқықтарын иемденуге мүмкіндік береді.

Мысал: Сервер JWT қолтаңбасын тексермесе, шабуылдаушы токенді өзгертіп, өзіне жоғары рұқсаттар тағайындай алады.

6. Man-in-the-Middle (MITM) - шабуылдаушы пайдаланушы мен сервер арасындағы деректер алмасуды ұстап алып, өзгерте алатын осалдық. Бұл ақпаратты ұрлау, жалған деректер енгізу немесе зиянды кодты енгізу үшін қолданылады.

Мысал: WebSocket қосылымы қорғалмаса, шабуылдаушы хабарламаларды ұстап, өзгерте алады, мысалы, ақша аударым сомасын арттыру.

7. DoS/DDoS шабуылы - жүйені немесе қызметті шамадан тыс жүктеу арқылы оны заңды пайдаланушылар үшін қолжетімсіз етуге бағытталған шабуылдар. DoS-шабуылдар бір көзден жасалса, DDoS-шабуылдар бірнеше таралған көздерден орындалады, бұл оларды тоқтатуды қиындатады.

Мысал: Шабуылдаушы серверге мыңдаған WebSocket қосылымдарын ашып, оның ресурстарын сарқып, қызметін істен шығара алады.

8. Бизнес-логика осалдықтары - қолданба логикасындағы қателіктер, олар шабуылдаушыларға жүйедегі процестерді өз пайдасына бұрмалауға, шектеулерді айналып өтуге немесе рұқсат етілмеген ресурстарға қол жеткізуге мүмкіндік береді.

Мысал: WebSocket API қате конфигурацияланған жағдайда, шабуылдаушы жүйені айланып өтіп, рұқсат етілмеген операцияларды орындай алады.

Осалдықтарды және олардың ықтимал салдарын терең түсіну ұйымдарға қауіпсіздікті күшейтіп, тәуекелдерді төмендету үшін алдын алу шараларын қабылдауға мүмкіндік береді.

1-Кесте Осалдықтарды салыстыру

№	Осалдықтар	Мақсаты	Әсері	Қауіпі	Алдын алу
1	Аутентификация мен авторизацияның болмауы	Жүйеге рұқсатсыз кіру	Шабуылдаушы басқа қолданушының сессиясын иемдене алуы	Жоғары	WebSocket сессиясында аутентификацияны талап ету, токендерді тексеру
2	Деректерді ашық түрде беру	Деректерді ұрлау	Құпия ақпарат желіде ашық беріледі және ұстап қалынуы мүмкін	Жоғары	wss:// пайдалану, TLS шифрлауын қосу
3	SQL-инъекция және командалық инъекция	Дерекқорға рұқсатсыз қол жеткізу	Деректерді өзгерту немесе жою, жүйені зақымдау	Жоғары	Кіріс деректерді сүзу, SQL-инъекцияға қарсы қорғау (prepared statements)
4	XSS	Код енгізу арқылы пайдаланушыны алдау	Жеке деректерді ұрлау, пайдаланушы әрекеттерін бақылау	Орташа	Сервер тарапынан енгізілген деректерді экранизациялау (sanitization)
5	JWT немесе сессия токендерін ұрлау	Токендерді өзгерту арқылы артық рұқсаттар алу	Шабуылдаушы өзіне әкімші рұқсатын тағайындай алу	Жоғары	Токендерді шифрлау, қолтаңбаларды тексеру, қысқа өмірлік цикл орнату
6	MITM	Байланысты ұстап, өзгерту	Қолданушының төлемдері мен хабарламаларын өзгерту	Жоғары	TLS пайдалану, HSTS енгізу, сертификат тексеру
7	DoS/DDoS-шабуылы	Қызметті істен шығару	Сервер ресурстарын сарқып, жүйені бұғаттау	Орташа	WebSocket қосылымдарының санын шектеу, rate limiting қолдану
8	Бизнес-логика осалдықтары	Қорғауды айналып өту	Рұқсатсыз транзакциялар, деректерге заңсыз қол жеткізу	Орташа	Қауіпсіздік аудиті, дұрыс авторизация және аутентификация механизмдері

Осалдықтарды анықтау үшін әртүрлі әдістер мен құралдар қолжетімді, олардың әрқайсысының өз артықшылықтары мен шектеулері бар

2-Кесте Осалдықты анықтау әдістерін салыстыру

Әдіс	Сипаттамасы	Артықшылықтары	Кемшіліктері	WebSocket осалдықтарына мысал
Статикалық талдау (SAST)	WebSocket байланысын өңдейтін кодты талдау	Ерте кезеңде қателерді анықтау, автоматтандыру	Эксплуатациялық осалдықтарды таба алмайды	WebSocket өңдеушілерінің қорғалмауы, деректерді тексеру қателері
Динамикалық талдау (DAST)	Жұмыс істеп тұрған WebSocket протоколын тестілеу	Осалдықтарды автоматты түрде анықтау	Өзара әрекеттесу логикасын толық тексере алмайды	WebSocket хабарламаларын ауыстыру, деректердің таралуы
Фаззинг (Fuzzing)	WebSocket арқылы кездейсоқ немесе арнайы жасалған деректерді жіберу	Деректерді өңдеу кезіндегі қателерді анықтау	Жоғары есептеу ресурстарын талап етеді, баптауды қажет етеді	WebSocket арқылы DoS шабуылдары, буферді асыра толтыру
Пентест	WebSocket қосылымдарына қарсы нақты шабуылдарды модельдеу	Қауіпсіздіктің нақты жағдайын бағалау	Жоғары білікті мамандарды қажет етеді	WebSocket деректерін өзгерту, аутентификацияны айналып өту
Сканерлеу	WebSocket-тегі белгілі осалдықтарды автоматты түрде іздеу	Стандартты осалдықтарды жылдам анықтау	Жалған іске қосулар болуы мүмкін, бірегей осалдықтарды таппайды	Жалған сұраныстардан қорғаныстың (CSRF) болмауы, WebSocket-ке енгізу шабуылдары

Қортынды

Интернет-ресурстардың өмірімізге біртіндеп енгізілуі қызметтер мен кеңес алуда үлкен артықшылықтарды береді. Веб-қосымшалардың функционалдық дамуы қауіпсіздікті сапалы қамтамасыз етумен қатар жүруі тиіс. Қосымшалардың қауіпсіздігін қамтамасыз етуде қауіп төндіретін мәліметтер жиынтығынан тұратын базалардың маңызы зор. Зерттеу қорытындысында WebSocket пайдаланатын веб-қосымшалардың қауіпсіздігі ақпараттың құпиялылығын, тұтастығын және қол жетімділігін сақтау үшін өте маңызды екенін анықтадық. Соңғы жылдары WebSockets танымалдылығының артуы оларды пайдалануды екі есеге арттырды, бұл оларды кибершабуылдар үшін тартымды нысанаға айналдыруда. Біздің жұмысымыз веб-қосымшалардың қауіпсіздігін қамтамасыз етудің кешенді тәсілінің маңыздылығын көрсетеді.

Зерттеу негізінде websocket технологиясын қолданатын веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін бірқатар ұсыныстар жасауға болады:

- TLS/SSL пайдалану: барлық WebSocket қосылымдары деректердің құпиялылығы мен тұтастығын қамтамасыз ету үшін шифрланған арналарды (wss://) пайдалану;
- Сайтаралық сценарийден қорғау (XSS): пайдаланушы енгізуін санитариялау, Content Security Policy (CSP) қауіпсіздік тақырыптарын орнату және басқа шаралар арқылы XSS-тің алдын алу;
- CSRF шабуылдарынан қорғау: веб-пішіндер мен басқа күйді өзгертетін сұраулар үшін CSRF шабуылдарына қарсы белгілерді пайдалану;
- Аутентификация және авторизация: OAuth, JWT немесе HTTP-Only және Secure cookie сеанстарын пайдалануды қоса алғанда, барлық кезеңдерде сенімді аутентификация мен авторизацияны қамтамасыз ету;

Пайдаланылған дереккөздердің тізімі

1. WebSocket: Lightweight Client-Server Communications, Andrew Lombardi 2015, 141p
2. The Definitive Guide to HTML5 WebSocket, Frank Salim Peter Moskovits, 2013, 227 p
3. https://cyberleninka.ru/article/n/kak-ispravit-mezhsaytovuyu-uyazvimost-web-socket
4. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9182458
5. https://book.hacktricks.xyz/pentesting-web/websocket-attacks
6. https://medium.com/swlh/hacking-websocket-25d3cba6a4b9
7. https://portswigger.net/web-security/websockets
8. https://ably.com/topic/websocket-security
9. https://www.shodan.io/
10. https://datatracker.ietf.org/doc
11. https://infosecwriteups.com/cross-site-websocket-hijacking-cswsh-ce2a6b0747fc/html/rfc6455
12. https://infosecwriteups.com/cross-site-websocket-hijacking-cswsh-ce2a6b0747fc

УДК 004.056

АВТОМАТИЗАЦИЯ ПРОЦЕССА АНАЛИЗА ОПЕРАТИВНОЙ ПАМЯТИ С ИСПОЛЬЗОВАНИЕМ PYTHON

Майданов Алихан Серикович
Alikhan.m.01@gmail.com
Магистрант кафедры Информационная безопасность ЕНУ им. Л.Н. Гумилева, Астана, Казахстан Астана, Казахстан
Научный руководитель – Ахметова Ж.Ж.

Аннотация. В данной работе будет рассмотрен **Volatility Framework** и его ключевые возможности, связанные с анализом оперативной памяти. Будут продемонстрированы примеры использования плагинов, связанных с выявлением аномалий в процессах, закрепившихся в оперативной памяти, анализ подгруженных dll-файлов и их указателей, а также исследование оперативной памяти на предмет внедренного кода. Более того, в данной статье рассмотрены правила Yara Rules, а также скрипты на Python, позволяющие автоматизировать процесс анализа памяти. Результатом исследования станет создание набора автоматизации на базе Python, которые позволят автоматизировать рутинные задачи по анализу оперативной памяти, для ускорения процесса расследования кибератак и повышения его точности.