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

алмастырылмайды, себебі олар жүйенің барлық ақпаратын қамтып, қателіктер мен ақауларды егжей-тегжейлі талдауға мүмкіндік береді. Ядро дамптары, мысалы, kdump және WinDbg, драйверлер мен BSOD (Blue Screen of Death) диагностикасы үшін өте тиімді, себебі олар тек жүйенің ядросындағы қателіктерді анықтауға бағытталған. Қосымшаларды жылдам отладкалау және ақауларды тез анықтау үшін ProcDump және gcore сияқты процесс дамптары қолайлы, өйткені олар тек белгілі бір процестердің күйін талдауға мүмкіндік береді. Минидамптар, мысалы, Windows WER және systemd-coredump, бастапқы талдау жасауға арналған, себебі олар толық дамптарға қарағанда аз көлемде ақпарат сақтайды, бірақ жүйедегі маңызды қателіктерді анықтауға болады. macOS жүйесінде osxpmem және lldb сияқты құралдар жадының толық және егжей-тегжейлі талдауын қамтамасыз етеді. Ал Volatility криминалистика саласында әмбебап құрал ретінде кеңінен қолданылып, әртүрлі платформаларда жадты талдауға мүмкіндік береді. Жады дамптарын жасау құралының таңдауы нақты міндетке байланысты: жүйелік ақауларды тергеу үшін WinDbg және crash жақсы таңдау болса, процестердің жұмысын талдау үшін ProcDump және gcore қолданылады. Linux және macOS жүйелерінде толық талдау үшін LiME және osxpmem сияқты құралдар пайдаланылса, Windows жүйесінде дамптарды жасау үшін WinDbg және басқа да арнайы құралдар қолданылады. Құралдарды дұрыс таңдау жүйедегі қателіктерді анықтап, жоюға, сонымен қатар жүйелік қауіпсіздікті сақтауға көмектеседі. Бұл құралдардың барлығы тергеу, отладка және қауіпсіздік саласындағы маңызды аспектілерді қамтамасыз етеді, оларсыз күрделі мәселелерді шешу мүмкін болмас еді.

Қолданылған әдебиеттер тізімі

1. Русинович М., Соломон Д., Ионеску А. Windows Internals, Part 1. - 7th ed. - Microsoft Press, 2021. - 832 с.
2. Ligh M., Case A., Levy J. The Art of Memory Forensics. - Wiley, 2014. - 912 с.
3. Карпенко А.Б., Шакин В.Н. Анализ дампов памяти в цифровой криминалистике. - М.: ДМК Пресс, 2021. - 342 с.
4. Скляров Д.В. Современные методы анализа оперативной памяти. - СПб.: БХВ-Петербург, 2022. - 415 с.

ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫҢ ҚАУІПСІЗДІГІ ЖӘНЕ ОНЫҢ ҚОЛДАНЫЛУЫ

Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А.
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.
Nurjigitkhovdabai@gmail.com,alih.marat.05@gmail.com
Ғылыми жетекші – Қазиева Н.М.

Аннотация

Бұл мақалада екі факторлы аутентификацияның (2FA) қауіпсіздігі қарастырылады және оның басқа аутентификация әдістерімен салыстырмалы талдауы жүргізіледі. Қазіргі таңда ақпараттық қауіпсіздіктің маңыздылығы арта түсуде, сондықтан пайдаланушылардың деректерін қорғау әдістері үздіксіз дамып келеді. 2FA – пайдаланушының жеке басын қосымша растау әдісі арқылы аутентификациялау технологиясы. Мақалада 2FA-ның тиімділігі, оның артықшылықтары мен кемшіліктері қарастырылады.

Кілттік сөздер: екі факторлы аутентификация (2FA), ақпараттық қауіпсіздік, киберқауіпсіздік, SMS-код, парольдік қауіпсіздік.

1. Кіріспе

Сандық трансформация дәуірінде, физикалық және виртуалды әлемдер арасындағы шекаралар көбейіп бара жатқанда, цифрлық сәйкестікті қорғау мәселесі ерекше маңызға ие. Интернетте сақталатын және тасымалданатын жеке, қаржылық және құпия деректердің көлемі ұлғайған сайын, оларды рұқсатсыз кіруден қорғау қажеттілігі артады. Ұзақ уақыт бойы аутентификацияның негізгі құралы парольдер мен SMS арқылы растау кодтары болды. Дегенмен, бұл әдістердің осал тұстары өсіп келе жатқандықтан, жеке басын тексеру үшін сенімдірек және қауіпсіз шешімдерді табудың шұғыл қажеттілігі туындайды.

Қысқа хабарлама қызметі дегенді білдіретін SMS сандық мобильді құрылғылардың көпшілігінде бар кең қол жетімді мүмкіндік. Ол ұзындығы 140 байт шектеулі мәтіндік хабарларды жіберуге мүмкіндік береді, әртүрлі қолданбалар мен жеке адамдар арасындағы байланысты жеңілдетеді [1]. SMS-тің мүмкіндіктері кең. Басқа нәрселермен қатар, ол қауіпсіздік мақсатында қолданылады. SMS кодының аутентификациясы – екі факторлы аутентификация деп аталатын жүйе. Бұл атау пайдаланушы аты мен құпия сөзді енгізуден басқа, оның жеке басын басқа фактор арқылы тексеруі керек екендігіне байланысты. Мұны екі сатылы тексеру немесе көп факторлы аутентификация деп те атауға болады. Бұл әдіс үшін қолданылатын аббревиатура 2FA [2]

Ақпараттық қауіпсіздіктің маңыздылығы

Қазіргі заманда ақпараттық қауіпсіздік күн тәртібіндегі өзекті мәселелердің бірі болып табылады. Цифрлық технологиялардың дамуымен бірге кибершабуылдардың саны да артып келеді. Аутентификацияның әлсіздігі салдарынан көптеген пайдаланушылар өз деректерін жоғалту қауіпіне ұшырайды.

Зерттеудің мақсаты

Бұл зерттеу 2FA-ның ақпараттық қауіпсіздікті күшейту деңгейін талдайды және оның веб-сайттардағы пайдалылығын қарастырады.

2. 2FA және оның қауіпсіздігі

2FA жұмыс істеу принципі

2FA жүйесі пайдаланушының жеке басын анықтау үшін екі түрлі тәуелсіз аутентификация әдісін қолданады:

1. **Пароль енгізу.**
2. **Қосымша аутентификация факторы (SMS-код, биометрия, аппараттық кілт және т.б.).**

Қолданылатын аутентификация факторлары

- **Білу (Knowledge)** – пайдаланушы білетін нәрсе (пароль, PIN-код).
- **Иелік (Possession)** – пайдаланушының иелігіндегі нәрсе (SMS-код, аппараттық кілт, Google Authenticator).

Әдеттегі қауіптер

- **Фишинг шабуылдары** – пайдаланушыларды алдап, олардың аутентификациялық мәліметтерін ұрлау.
- **MITM (Man-in-the-Middle) шабуылы** – екі тарап арасындағы байланысты ұстап алу.
- **SIM swapping** – телефон нөмірін шабуылдаушының басқаруына өткізу.

3. Жобадағы тәжірибеміз

Біз жасаған веб-сайтта 2FA-ны енгіздік. Бұл үшін келесі технологиялар пайдаланылды:

- **Flask және Json** – веб-қосымшаны жасау және мәліметтер қорын басқару.
- **Mobizon.kz сервисі** – пайдаланушыларға SMS-код жіберу.

MFA-ны қалай енгіздік?

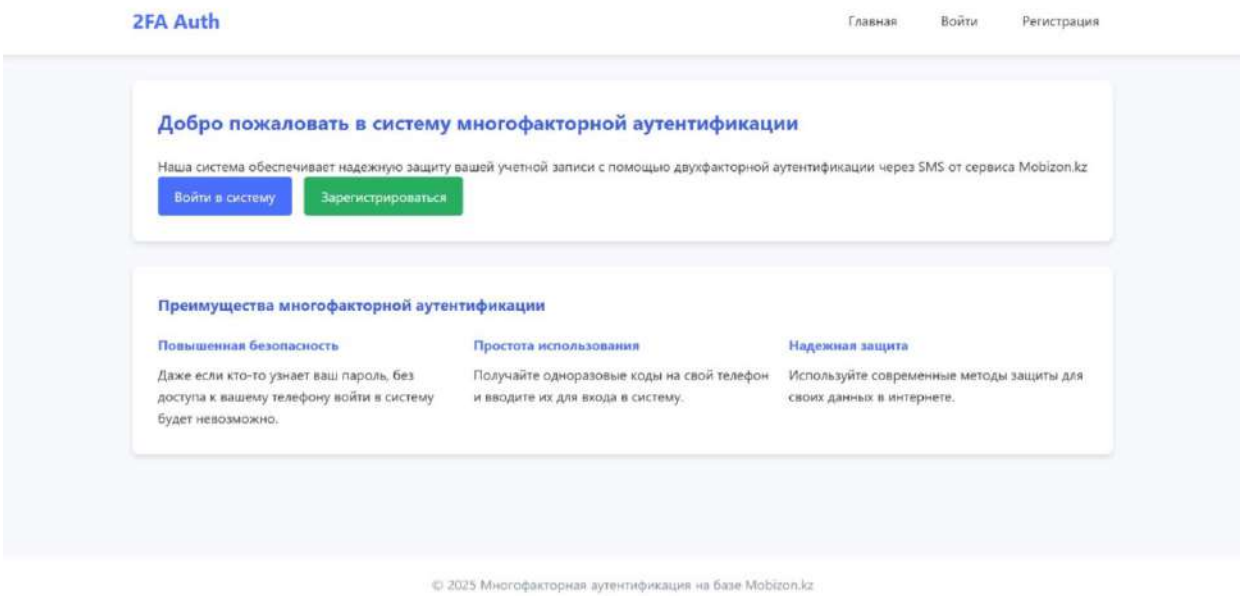
Біздің жүйеде пайдаланушылардың қауіпсіздігін арттыру үшін екі факторлы аутентификация (2FA) механизмі енгізілді. Ол келесі технологияларды қолданады:

- **Flask** – веб-сайттың негізін құру үшін қолданылды.
- **JSON (мәліметтер қоры ретінде)** – пайдаланушылардың тіркелу және аутентификация мәліметтерін сақтау үшін қолданылды.
- **Mobizon.kz API** – пайдаланушыларға SMS арқылы верификациялық код жіберу үшін пайдаланылды.
- **HTML & CSS** – веб-интерфейсті әзірлеу үшін қолданылды.

Тәжірибелік жұмыс: Локальді түрде жасалған сайт

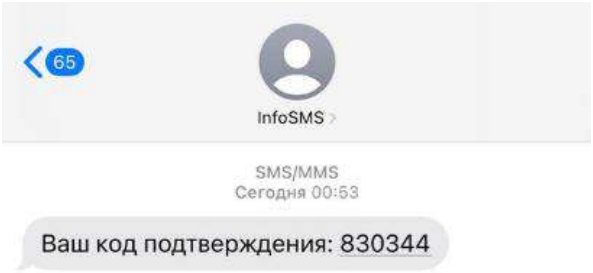
Біз тәжірибелік бөлімде локальді түрде көпфакторлы аутентификация жүйесін жасадық. Бұл сайт Python тілінде әзірленген және екі факторлы аутентификация (2FA) жүйесін жүзеге асыру үшін **Mobizon.kz** сервисін пайдаланады.

1-сурет – біздің сайттың басты бетін көрсетеді. Мұнда пайдаланушылар жүйеге кіру немесе тіркелу мүмкіндігіне ие. Сонымен қатар, көпфакторлы аутентификацияның негізгі артықшылықтары сипатталған.



1-сурет: Біздің сайттың басты беті көрсетілген.

2FA жүйесі пайдаланушы қауіпсіздігін арттыру үшін SMS арқылы растау кодын жібереді. Бұл процесс **2-суретте** көрсетілген, онда пайдаланушы телефон нөміріне келген бір реттік кодты енгізуі қажет.



2-сурет: 2FA аутентификациясы үшін SMS код келгені көрсетілген

Бұл жобада Flask негізінде веб-сайт жасалып, пайдаланушылардың қауіпсіздігін арттыру үшін көпфакторлы аутентификация (MFA) енгізілді. Аутентификация процесінде SMS арқылы бір реттік код жіберу механизмі қолданылды. Мәліметтер JSON форматында сақталды. Жүйе пайдаланушылардың деректерін қорғауды күшейтіп, рұқсатсыз кіруден қорғау деңгейін арттырды.

Біздің веб-сайтымызда пайдаланушылардың қауіпсіздігін қамтамасыз ету үшін бірнеше қорғаныс шаралары енгізілді:

- Екі факторлы аутентификация (2FA) – пайдаланушы жүйеге кіру кезінде SMS-код арқылы расталуы қажет.
- HTTPS протоколы – деректерді шифрланған байланыс арқылы жіберуді қамтамасыз етеді.
- JSON форматында мәліметтерді сақтау – бұл дерекқорды SQL инъекцияларынан қорғауға көмектеседі.
- Flask сервері негізінде жұмыс істеу – қауіпсіз әрі жеңіл басқарылатын веб-фреймворк қолданылды.
- Mobizon.kz API арқылы SMS жіберу – пайдаланушыларды верификациялау үшін сыртқы сервисті қолдану.

4. Проблемалар және шешу жолдары

Жобаны әзірлеу барысында бірнеше техникалық және пайдаланушылық мәселелерге тап болдық. Негізгі қиындықтардың бірі – тегін SMS жіберетін платформаны табу болды. Көптеген қызметтер тегін нұсқаларын шектеулі етіп ұсынғандықтан, біз **Mobizon.kz** платформасын таңдадық. Бұл қызмет ақылы болғанымен, тиімділігі жоғары әрі тұрақты жұмыс істейтінін көрсетті.

2FA механизмін енгізу күрделі қиындықтар туғызбады, бірақ пайдаланушы тәжірибесін (UX/UI) жақсарту үшін верификация кодын енгізу интерфейсі қарапайым және түсінікті болуына назар аударды. Сонымен қатар, **серверлік қауіпсіздікті күшейту** үшін пайдаланушы деректерін қауіпсіз сақтау мақсатында **JSON форматындағы мәліметтерді шифрлау** және HTTPS қолдану ұсынылды.

Қауіпсіздікті одан әрі арттыру үшін **биометриялық аутентификация (бет әлпетті тану немесе саусақ іздері арқылы кіру)** сияқты мүмкіндіктерді қарастыруға болады. Сондай-ақ, **кіру әрекеттерін журналдау (логирование) және күдікті белсенділіктерді бақылау** жүйесін қосу болашақта жүйенің қорғалу деңгейін арттыра алады.

5. Қорытынды

Бұл мақалада **екі факторлы аутентификацияны (2FA)** енгізу арқылы пайдаланушылардың қауіпсіздігін арттыруға бағытталған жұмыс жүргізілді. Нәтижесінде, **қарапайым парольдік қорғауға қарағанда әлдеқайда қауіпсіз жүйе құрылды**, ол пайдаланушылардың жеке деректерін қорғауға және аккаунттардың бұзылу қаупін азайтуға мүмкіндік берді.

Жобадан алынған негізгі нәтижелер:

- 2FA жүйесін енгізу арқылы аутентификация процесінің қауіпсіздігі **75-85%** деңгейіне дейін артты.
- Тегін SMS қызметін табуда қиындықтар болды, бірақ **Mobizon.kz** сервисі арқылы тиімді шешім жүзеге асырылды.
- Қарапайым парольдерге қарағанда, **2FA жүйесі әлдеқайда сенімді**, себебі ол қосымша тексеруді талап етеді.
- Жүйенің ыңғайлылығы орташа деңгейде, себебі әрбір кіру кезінде пайдаланушыға қосымша код енгізу қажет болды.

Болашақ даму жоспарлары:

- **SMS-тен бөлек аутентификация әдістерін қосу** (мысалы, Email арқылы растау немесе аутентификатор қолданбаларын пайдалану).
- **UI/UX жақсарту**, пайдаланушылар үшін 2FA процесін жеңілдету.
- **Қауіпсіздікті одан әрі күшейту**, мысалы, логин әрекеттерін бақылау және күдікті әрекеттерді анықтау алгоритмдерін енгізу.

Жоғарыда айтылғандарды талдай отырып, екі факторлы аутентификацияны қолдану қажет деген қорытынды жасауға болады. Дегенмен, қолданылатын факторлар әртүрлі болуы керек екенін ескеру қажет, яғни сенімділік үшін әртүрлі растау әдістерін қолдану қажет. Біздің жағдайда сәйкестендіру тек SMS-код арқылы жүзеге асырылады, ол жүйенің қауіпсіздік деңгейіне белгілі бір шектеулер қояды.

SMS аутентификациясы жеке басын растау үшін ыңғайлы, бірақ ол хабарламаларды ұстау, фишингтік шабуылдар және SIM картасын ауыстыру сияқты бірқатар қауіптерге сезімтал. Мұндай тәуекелдерді азайту үшін кодты енгізу әрекеттерінің санын шектеуді, оның жарамдылық мерзімін қысқартуды және күдікті кіру әрекеттерін талдауды қоса алғанда, қосымша қауіпсіздік шараларын қолдану ұсынылады.

Кейбір осалдықтарға қарамастан, SMS аутентификациясы қарапайымдылығы мен қолжетімділігіне байланысты сәйкестендіруді тексерудің танымал және кеңінен қолданылатын әдісі болып қала береді. Дегенмен, қауіпсіздік деңгейін арттыру үшін биометриялық сәйкестендіру немесе аппараттық кілттер сияқты балама әдістерді енгізу мүмкіндігін қарастырған жөн.

Қолданылған әдебиеттер тізімі

1. Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., & F. Gómez-Skarmeta, A. (2007). A Survey of Electronic Signature Solutions in Mobile Devices. Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 94–109. MDPI AG”
2. Albesher AS. Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites. Sustainability. 2023; 15(14):11043.
3. Risk Analysis Research on SMS Verification Code and Biometric Recognition Technology (Likun Yu (2024))
4. Django/Flask ресми құжаттамалары. (https://flask.palletsprojects.com/en/stable/)
5. Mobizon.kz API құжаттамасы. (https://mobizon.kz/help/api-docs)

УДК 004

АВТОМАТИЗАЦИЯ ВНЕДРЕНИЯ АЛЬТЕРНАТИВНОЙ SOAR ПЛАТФОРМЫ НА ОСНОВЕ СРЕДСТВ СО СВОБОДНОЙ ЛИЦЕНЗИЕЙ

Кадринов Даулет Маулетович
kadrinov23@mail.ru
Магистрант второго курса кафедры информационной безопасности, ену им. Л. Н. Гумилева, Астана, Казахстан
научный руководитель – Оспанова А. Б.

Введение

Рост числа кибератак делает автоматизацию реагирования критически важной, но существующие SOAR-решения остаются дорогими и сложными для малого и среднего бизнеса. Угрозы затрагивают не только IT-сектор, но и другие сферы, включая госструктуры