

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

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

ISBN 978-601-08-5373-7

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

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

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

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

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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

| | | |
|------|--|-----|
| | инновациялық тәсілдері туралы» | |
| 220. | Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика» | 874 |
| 221. | Жаңабекқызы А. «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. «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 |

Пайдаланылған әдебиеттер тізімі

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2012. – 960 с. [https://kr-labs.com.ua/books/Tenenbaum_KS.pdf]
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – 2-е изд. – М.: Триумф, 2006. – 816 с. [https://kr-labs.com.ua/books/Bryus_Shnayer_-_Prikladnaya_Kriptografiya.pdf]
3. Лапонина О.Р. Основы сетевой безопасности. – Национальный Открытый Университет «ИНТУИТ», 2014. – 384 с [<http://master.cmc.msu.ru/files/Laponina-1.pdf>]
4. Kurose J., Ross K. Computer Networking: A Top-Down Approach. – 7th ed. – Pearson, 2017. –912p. [https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20%20A%20Top%20Down%20Approach,%207th,%20converted.pdf]
5. Kali Linux операциялық жүйесі [<https://www.kali.org/get-kali/#kali-platforms>]
6. NMAP утилитасы [<https://nmap.org/download>]
7. Telegram әлеуметтік желісі [<https://web.telegram.org/>]

ФИШИНГ: ЖЕЛДЕГІ ВЕЕФ ӘДІСІ АРҚЫЛЫ АЛДАУ ЖӘНЕ ОДАН САҚТАНУ

Таубай М.Е. Раматуллаев Ә.А.

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

maditaubay04@gmail.com alimramatullaev@gmail.com

Аңдатпа

Бұл мақалада біз сілтеме арқылы шабуыл жасау түрлерін қарастырамыз. Біздің қарастыратындарымыз фишинг және ВеЕФ (Browser Exploitation Framework), сондай-ақ екеуінің өзара байланысын және осы қауіптерден қорғану әдістерін талдаймыз. Хакерлердің ВеЕФ-ті қалай өздеріне тиімді етіп пайдаланатынын және пайдаланушылар мен ұйымдардың осы шабуылдарға төтеп бере алатындай қандай қадамдар жасайтынын талқылаймыз.

Кілттік сөздер: фишинг, әлеуметтік инженерия, ВеЕФ, интернет қауіпсіздігі, киберқауіп, қорғаныс әдістері.

1. Кіріспе

Интернеттегі қауіптер күн сайын күрделене түсуде, ал киберқылмыскерлер пайдаланушылардың жеке деректерін алу үшін жаңа әдістерді қолдануда. Солардың ішінде ең көп тарағаны – **фишинг**. Бұл – алаяқтықтың кең таралған түрі, оның көмегімен қаскүнемдер логиндер, парольдер, банк карталарының деректері сияқты маңызды ақпаратты қолға түсіреді. Сонымен қатар, **ВеЕФ (Browser Exploitation Framework)** құралы веб-шолғыштардың осалдықтарын пайдаланып, шабуылдаушыларға қосымша артықшылықтар береді.[1]

Фишингтің қаупі

Фишингтің басты қаупі – оның адамдарды алдау арқылы жүзеге асуы, сондықтан одан толық қорғану қиын. Компаниялар ақпараттық қауіпсіздік бойынша оқыту жүргізсе де, алаяқтар өз әдістерін жетілдіріп отырады.

Фишингтің тағы бір қатері – құпия деректердің қолды болуы. Егер **логин мен құпиясөз** ұрланса, қолданушы аккаунтынан айырылуы мүмкін. **Банк картасының мәліметтері** түссе, алаяқтар қаржыны иемденуге тырысады. Ал жеке ақпарат көбіне **үшінші тараптарға сатылады, интернетте жарияланады** немесе **қосымша шабуылдарға қолданылады**. [2]

Бұл мақалада фишинг түрлері, ВеЕF-тің жұмыс істеу принциптері және осындай шабуылдардан қорғану әдістері қарастырылады.

Фишинг түрлері және әдістері

Фишинг – кибершабуыл түрі, онда зиянкестер пайдаланушыларды құпия сөздер, несие картасы деректері немесе корпоративтік жүйелерге қол жеткізу сияқты құпия ақпаратты беру үшін алдайды. Фишинг әлеуметтік инженерияға негізделген: шабуылдаушылар жалған электрондық хаттар, веб-сайттар немесе әлеуметтік медиа хабарламалар жасау арқылы сенімді адамдар немесе ұйымдар ретінде жасырылады.[3]

1. **Email-фишинг** – Фишерлер жалған электрондық хаттарды жібереді, пайдаланушыларды алдап, оларды зиянды сілтемеге өту сияқты жеке ақпаратты ашуға тырысады. [3]

2. **Spear phishing (нысаналы фишинг)** – бұл әдеттегі фишингтің жекелендірілген нұсқасы. Жаппай жіберудің орнына зиянкестер белгілі бір адамдарды немесе компанияларды таңдайды. Олар өз хабарламаларын мүмкіндігінше сенімді және сенімді ету үшін әлеуметтік желілер немесе басқа қол жетімді көздер арқылы өз мақсаттары туралы ақпаратты алдын ала жинай алады. [3]

3. **Vishing (Voice phishing)** – бұл телефон қоңыраулары арқылы жасалатын фишинг. Алаяқтар пайдаланушыларға қоңырау шалып, банк карталарының құпия деректерін, жүйелерден логиндерді немесе басқа ақпаратты алу үшін банк, қауіпсіздік, техникалық қолдау қызметкерлерімен таныстырады. Көбінесе шабуылдаушылар нөмірлерді ауыстыру технологиясын қолданады, бұл сізге сенімді ұйымдардың қоңырауларына ұқсас қоңыраулар жасауға мүмкіндік береді. [3]

4. **Smishing (SMS phishing)** – бұл алаяқтар SMS хабарламаларын қолданатын фишингтің бір түрі. Электрондық пошта алаяқтығы сияқты, шабуылдаушылар мәселені шешу үшін сілтемеге өтуді немесе нөмірге қоңырау шалуды ұсынатын жалған хабарламалар жібереді. [3]

5. **Whaling** ("үлкен балықты" аулау) – бұл компанияның жоғары лауазымды тұлғаларына бағытталған spear-фишингтің бір түрі: мысалы, бас және қаржы директорлары. Шабуылдар мұқият ойластырылуы мүмкін, өйткені мұндағы ставкалар әлдеқайда жоғары.[3]

Мақалада ВеЕF және оның қолданылуын қарастырылды, айта кетсек ВеЕF (Browser Exploitation Framework) – веб-шолғыштардың осалдықтарын анықтау және оларды пайдалану үшін жасалған құрал. Бастапқыда бұл фреймворк ақпараттық қауіпсіздік мамандары үшін тестілеу мақсатында әзірленсе де, кейіннен оны хакерлер мен алаяқтар да белсенді қолдана бастады.

ВеЕF қалай жұмыс істейді?

1. **Жәбірленушіні шабуылға ұшырату** – пайдаланушы зиянды сілтемеге өтеді немесе шабуылдаушы арнайы код енгізілген сайтқа кіреді.

2. **Шолғыштың осалдығын пайдалану** – ВеЕF арқылы шабуылдаушы пайдаланушының браузеріне қосылып, оған түрлі командалар жібере алады.

3. **Деректерді ұрлау** – шабуылдаушы құрбанының сессия мәліметтерін, cookie-файлдарын, сақталған парольдерін және басқа да жеке ақпараттарын жинай алады.

4. **Құрылғыны басқару** – кейбір жағдайларда шабуылдаушы жәбірленушінің құрылғысын қашықтан бақылап, веб-камераны қосу, пернетақта әрекеттерін тіркеу және сайттарға автоматты түрде қайта бағыттау сияқты әрекеттерді орындай алады.[4]

Қорғаныс әдістері

Зерттеу барысында келесі қорғаныс әдістері қарастырылды:

1.Браузер қауіпсіздігін қамтамасыз ету

- **Браузерді жаңарту:** зерттеу кезінде браузердің соңғы нұсқасын пайдалану қажеттілігі талданды. Сонымен қатар, осалдықтарды жоятын патчтарды уақытылы орнатудың маңыздылығы атап өтілді.

2. Желілік қауіпсіздікті күшейту

- **VPN және прокси-серверлерді қолдану:** IP-мекенжайды жасыру және қосымша шифрлау деңгейін қамтамасыз ету арқылы желілік қауіпсіздікті арттыру әдістері зерттелді.

- **Қауіпті сайттарды бұғаттау:** желілік әкімшілеу құралдарын пайдалану арқылы белгісіз немесе күдікті сайттарға кірудің алдын алу мүмкіндігі қарастырылды.

3. Зиянды скрипттерден қорғау

- **JavaScript-ті шектеу:** зерттеу барысында белгісіз сайттарда JavaScript-ті өшіру әдістері қарастырылып, тек сенімді көздерден ғана скрипттерді орындауға рұқсат беру қажеттілігі анықталды.

- **Қауіпті браузер сессияларын болдырмау:** HTTPS қосылымдарын ғана пайдалану және белгісіз Wi-Fi желілерінде жұмыс істемеу арқылы қауіпсіздікті қамтамасыз ету жолдары қарастырылды.

4. Қолданушыларды оқыту және қауіпсіздік мәдениетін дамыту

- **Киберқауіпсіздік бойынша оқыту:** ВеЕF және басқа браузерлік шабуылдар туралы ақпараттандырудың маңыздылығы зерттелді. Сонымен қатар, қауіпсіздік саясатын енгізу қажеттілігі қарастырылды.

- **Ескертулер мен тестілеу:** персоналға әлеуметтік инженерия шабуылдарын анықтау бойынша тренингтер өткізу және браузерлік осалдықтарға тест жүргізу әдістері зерделенді.

Зерттеу нәтижесінде жоғарыда аталған қорғаныс шараларының тиімділігі талданып, оларды тәжірибеде қолдану мүмкіндіктері қарастырылды.[5]

Тәжірибелік жұмыс:

```
root@kali ~ # ./beef
[13:50:38][*] Browser Exploitation Framework (BeEF) 0.5.4.0
[13:50:38] |   | Twitter: @beefproject
[13:50:38] |   | Site: https://beefproject.com
[13:50:38] |   | Wiki: https://github.com/beefproject/beef/wiki
[13:50:38][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[13:50:38][*] BeEF is loading, wait a few seconds ...
[13:50:40][*] 7 extensions enabled:
[13:50:40] |   | XSSRays
[13:50:40] |   | Requester
[13:50:40] |   | Proxy
[13:50:40] |   | Network
[13:50:40] |   | Events
[13:50:40] |   | Demos
[13:50:40] |   | Admin UI
[13:50:40][*] 393 modules enabled.
[13:50:40][*] 2 network interfaces were detected.
[13:50:40][*] running on network interface: 127.0.0.1
[13:50:40] |   | Hook URL: http://127.0.0.1:3000/hook.js
[13:50:40] |   | UI URL: http://127.0.0.1:3000/ui/panel
[13:50:40][*] running on network interface: 10.0.2.15
[13:50:40] |   | Hook URL: http://10.0.2.15:3000/hook.js
[13:50:40] |   | UI URL: http://10.0.2.15:3000/ui/panel
[13:50:40][*] HTTP Proxy: http://127.0.0.1:8080
[13:50:40][*] RESTful API key: 7e11085387c1253040c88fd9ecads13bae3d52b
[13:50:40][*] BeEF server started (press control+c to stop)
```

1-сурет: ВеЕF серверін іске қосу

Бұл суретте біз Kali Linux терминалын ашып ВеЕF серверін іске қосу процесін көрсетеміз. **Hook URL:** Бұл URL-ге кірген браузер. Бұл браузерге шабуыл жасауға мүмкіндік береді. **UI URL:** Бұл ВеЕF басқару панеліне кіру үшін қолданылатын сілтеме. **HTTP Proxy:** ВеЕF басқа жүйелердің трафигін бақылауға арналған прокси қызметін де іске қосады. **RESTful API:** ВеЕF API арқылы сыртқы қосымшалардан командаларды орындауға мүмкіндік береді. Біз **ctrl** батырмасымен **UI URL** деп тұрған сілтемеге басамыз. Содан бізді сайтқа жібереді.



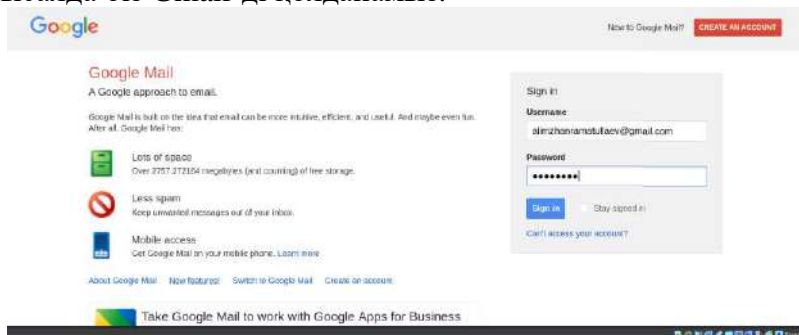
2-сурет: VeEF басқару панеліне кіру

Бұл суретте VeEF басқару панелінің кіру беті көрсетілген. Бұл жерде біз логин мен құпия сөзімізді теріп жүйеге кіреміз.



3-сурет: VeEF басқару панелі

VeEF басқару панелінің негізгі интерфейсі көрсетілген. Осы жерде бізге жүйеге кірген адамның IP адресі көрсетіледі. Содан кейін біз браузерге қосылған модулі бар терезені басып, Командалар және әлеуметтік инженерия қалтасынан Pretty Theft табыңыз және Орындау батырмасын басыңыз. Фишингтің әртүрлі әдістері бар, мысалы Facebook, LinkedIn және басқалары. Бұл мысалда біз Gmail-ді қолданамыз.



4-сурет: Фишинг (Pretty Theft модулі)

Бұл суретте жалған Google Gmail беті көрсетілген. Браузерде gmail почтасына кіру терезесіне ұқсайтын жалған форма пайда болады. Пайдаланушыдан электрондық пошта мен құпия сөзді енгізу сұралады. Бұл VeEF-тің **"Google Phishing"** модулі арқылы жасалған. Егер пайдаланушы логин мен құпия сөзін енгізсе, олар VeEF басқару панеліне жіберіледі.

| id | date | label |
|----|------------------|-----------|
| 0 | 2025-03-25 10:08 | command 1 |
| 1 | 2025-03-25 10:09 | command 2 |
| 2 | 2025-03-25 10:17 | command 3 |

| Command results |
|--|
| 1 data: result=Username: alimzhian@gmail.com Password: 12345678 |

5-сурет: Командалар және ұрланған деректер

ВеЕF басқару панеліндегі **Командалар** қойындысын көрсетеді. "**Module Tree**" : Мұнда браузерге жіберуге болатын әртүрлі шабуыл модульдері бар. Мысалы, "Pretty Theft," "TabNabbing," "Google Phishing" және т.б.

Қорытынды

Менің ойымша, қазіргі таңда фишинг – ең қауіпті кибершабуылдардың бірі болып табылады. Оны ВеЕF сияқты құралдар одан әрі күшейтіп, жеке адамдарға ғана емес, ірі ұйымдарға да зор зиян келтіруі мүмкін. Қорытындылай келе ВеЕF – браузер осалдықтарын пайдаланып, құрылғыны қашықтан басқаруға мүмкіндік беретін қауіпті құралдардың бірі. Бұл әдіспен шабуылдаушылар пайдаланушының сеансын бақылап, зиянды әрекеттерді орындай алады. Сондықтан ВеЕF шабуылдарынан қорғандың ең тиімді жолы – үнемі қырағылық танытып, қауіпсіздік шараларын дер кезінде қолдану. Әрбір қолданушы өз құрылғылары мен жеке деректерінің қауіпсіздігін қамтамасыз ету үшін интернеттегі қауіпсіздік ережелерін сақтап, қауіпсіздік жүйелерін жаңартып отыруы қажет.

Қолданылған әдебиеттер тізімі:

1. Митюков Е. А., Затонский А. В. Модель обнаружения фишинговых атак на основе гибридного подхода для защиты автоматизированных систем управления производством // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2020. №2 <https://cyberleninka.ru/article/n/model-obnaruzheniya-fishingovyh-atak-na-osnove-gibridnogo-podhoda-dlya-zaschity-avtomatizirovannyh-sistem-upravleniya-proizvodstvom>
2. Фишинг: ловись рыбка большая и маленькая [электронный источник, дата просмотра 19.05.2021] <https://habr.com/ru/companies/pentestit/articles/558138/>
3. <https://blog.skillfactory.ru/что-такое-fishing/> Какие бывают типы фишинга?
4. **Ronak Sharma, Phishing Attack Sample** [электронный источник, дата просмотра 19.03.2025] \\ <https://medium.com/@ronak.d.sharma111/phishing-attack-sample-8ff1260c680c>
5. Фишинговые письма: как их распознать и не стать их жертвой [//https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips](https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips)