

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. «Neuvector және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	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

оперативно выявлять уязвимости и предотвращать угрозы, включая методы сокрытия информации с использованием стеганографии. В мае 2024 года было утверждено постановление правительства, определяющее новые требования по обеспечению информационной безопасности. Среди них – использование систем для предотвращения утечек данных (DLP), а также внедрение фильтрации сетевого трафика с применением межсетевых экранов. Эти инструменты повышают уровень защиты от скрытых методов передачи информации.

Таким образом, Казахстан активно совершенствует кибербезопасность, принимая законодательные инициативы, внедряя современные технологии и взаимодействуя с международными организациями.

Стеганография — это мощный инструмент, который может использоваться как для защиты данных, так и в целях кибератак. Для Казахстана важно не только применять стеганографию в области информационной безопасности, но и разрабатывать методы её выявления и предотвращения вредоносного использования. Развитие технологий обнаружения, законодательное регулирование и повышение осведомленности специалистов помогут Казахстану эффективно противостоять киберугрозам, связанным со стеганографией. Внедрение новых технологий и активное сотрудничество государственных и частных компаний в сфере кибербезопасности позволит укрепить цифровую защиту страны и минимизировать риски, связанные с использованием стеганографии в преступных целях.

Список использованных источников:

1. Кибербезопасность. Учебник для вузов. – Санкт-Петербург: Издательство ЛАНЬ, 2024. – 680 с.
2. Стеганографические методы защиты информации. – Москва: Издательство Каргаслов, 2018. – 250 с.
3. Основы информационной безопасности и стеганографии: учебник и практическое руководство. – Казань: Издательство Казанского федерального университета, 2022. – 295 с.
4. Digital Watermarking and Steganography: Fundamentals and Techniques. – Boca Raton: CRC Press, 2017. – 292 p.

WI-FI ЖЕЛІСІНДЕ ШАҚЫРЫЛМАҒАН ҚОНАҚТАРДЫ АВТОМАТТЫ ТҮРДЕ АНЫҚТАУ ЖҮЙЕСІ

Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс

ttt.ernar@gmail.com, irgebaikliptonit@gmail.com, salikoalpalpamys@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті, Ақпараттық қауіпсіздік кафедре студенттері Танатаров Ернар, Іргебай Санжар, Султанов Алпамыс топ 39,39/1

Астана, Қазақстан

Ғылыми жетекшісі – Казиева Н.М.

Андатпа: Бұл мақалада Wi-Fi желісіндегі рұқсатсыз қосылған құрылғыларды автоматты түрде анықтау жүйесі қарастырылады. Жүйе желідегі құрылғыларды бақылап, белгісіз MAC-адресстерді сенімді құрылғылар тізімімен салыстырады. Егер рұқсат етілмеген құрылғы анықталса, әкімшіге Telegram API арқылы жедел хабарлама жіберіледі. Python және Scapy құралдарының көмегімен жүзеге асырылған бұл жүйе ARP және DHCP сұраныстарын пайдаланып, желідегі құрылғылардың белсенділігін талдайды. Сонымен қатар, Kali Linux негізінде қауіпсіздік тесттері жүргізіліп, желінің қорғаныс деңгейі бағаланады. Ұсынылған шешім ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға

бағытталған. Жүйенің функционалын кеңейту мақсатында болашақта жасанды интеллектті қолдану арқылы құрылғылардың мінез-құлқын талдау мүмкіндігі қарастырылады.

Түйін сөздер: Wi-Fi қауіпсіздігі, желі әкімшілігі, рұқсатсыз қосылу, шақырылмаған қонақтарды анықтау, ақпараттық қауіпсіздік, ARP сұранысы, DHCP сұранысы, MAC-адрес, Telegram API, Python, Scapy, желіні сканерлеу, ақ тізім, құрылғыны бұғаттау, Kali Linux, желілік қауіптер, кибершабуыл, Nmap, желілік мониторинг, қауіпсіздік тестілеуі.

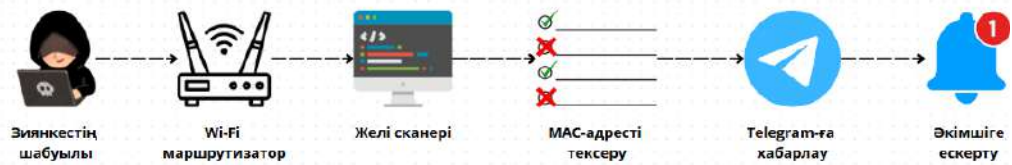
Қазіргі заманғы цифрлық ортада ақпараттық қауіпсіздікті қамтамасыз ету маңызды мәселелердің бірі болып табылады. Қауіпсіздік — бұл қашықтағы қызметтерге қол жеткізуге құқығы жоқ пайдаланушылардың оған талпынысын болдырмау[1, с. 807]. Цифрлық технологиялардың қарқынды дамуы және интернетке қосылу мүмкіндіктерінің кеңеюі ақпараттық қауіпсіздікке жаңа қауіптер туындатады. Соның ішінде, Wi-Fi желілерінің кең таралуы олардың қорғалу деңгейіне қойылатын талаптарды күшейтеді.

Wi-Fi желілері деректерді сымсыз тарату мүмкіндігі арқылы ыңғайлылық пен мобильділікті қамтамасыз етеді. Алайда, ашық және қорғалу деңгейі төмен Wi-Fi желілері кибершабуылдардың негізгі нысанасына айналады. Алаяқтар мұндай желілер арқылы пайдаланушылардың жеке деректеріне, банк карталарының мәліметтеріне және басқа да құпия ақпараттарына қол жеткізуі мүмкін. Wi-Fi желісіне белгісіз пайдаланушы кіріп кеткен жағдайда тіптен қиын болып кетеді, себебі ол сол әрекеті арқылы өзге пайдаланушылардың құйтырқы әрекеттеріне жол ашады. Интернет пайдаланушыларының адал екеніне сену — аңғалдық[2, с. 32]. Осыған байланысты шақырылмаған қонақтарды автоматты түрде анықтау жүйесін әзірлеу өзекті міндетке айналуда.

Бұл жүйе желідегі белсенді құрылғыларды бақылауға, рұқсатсыз қосылымдарды анықтауға және әкімшіге жедел хабарлама жіберуге мүмкіндік береді. Сонымен қатар, белгісіз құрылғыларды бұғаттау механизмі енгізіліп, желі қауіпсіздігін автоматтандыру шаралары қарастырылады. Жұмыс мысалыға MITM (Men in the middle) сияқты шабуылдармен Wi-Fi желісіне қосылмау үшін пайдалы қорғаныс түрі болуы мүмкін[3, с. 14]. Мұндай шешімдер ұйымдар мен жеке тұлғалар үшін Wi-Fi инфрақұрылымының қауіпсіздігін нығайтуға бағытталған. Жүйе Python және Scapy құралдарының көмегімен жүзеге асырылып, Telegram API арқылы хабарландырулар жіберу, iptables негізінде құрылғыларды бұғаттау және Kali Linux арқылы қауіпсіздік тесттерін жүргізу мүмкіндігін қамтиды. Бұл технологиялар кешені желіні қорғаудың тиімділігін арттырады және кибершабуылдарға қарсы тұрақтылығын қамтамасыз етеді. Желілік қауіпсіздік — бұл желі инфрақұрылымын және берілетін деректерді рұқсатсыз қол жеткізуден, шабуылдардан және істен шығудан қорғау практикасы [4, с. 657]. Ұсынылып отырған жүйе желіге рұқсатсыз қосылған құрылғыларды анықтап, олар туралы әкімшіні хабардар етуге арналған. Бұл келесі негізгі міндеттерді қамтиды:

1. **Желіде құрылғыларды анықтау** — ARP және DHCP сұраулары арқылы белсенді құрылғылардың MAC-адрестерін жинау.
2. **Ақ тізіммен салыстыру** — белгісіз MAC-адрестерді алдын ала анықталған сенімді құрылғылар тізімімен салыстыру.
3. **Хабарландыру жіберу** — Telegram бот арқылы әкімшіге күдікті құрылғылар туралы ескерту жіберу.

Сурет 1-де көрсетілген алгоритм жалпы Wi-Fi желісіне кіріп кеткен белгісіз пайдаланушыларды шығарып тастау процесін көрсетеді:



Сурет 1. Шақырылмаған қолданушыларды анықтау алгоритмі

```

1 import telebot
2 import os
3 import logging
4 from detect import scan_network, load_whitelist, get_vendor, get_device_info
5
6 # Настройки Telegram-бота
7 TOKEN = "7751411172:AAG0Zyx1i3oekNQOLM9RE0Em1iVZ98"
8 CHAT_ID = "-100275818"
9 bot = telebot.TeleBot(TOKEN)
10
11 # Настройка логирования
12 logging.basicConfig(filename="network_alerts.log", level=logging.INFO, format="%asctime)s - %(message)s")
13
14 # Файл заблокированных устройств
15 BLOCKED_FILE = "blocked_devices.txt"
16
17 def log_event(event):
18     """Записывает события в лог."""
19     logging.info(event)
20
21 def is_already_blocked(mac):
22     """Проверяет, был ли MAC-адрес уже заблокирован."""
23     if os.path.exists(BLOCKED_FILE):
24         with open(BLOCKED_FILE, "r") as f:
25             blocked_macs = f.read().splitlines()
26             return mac in blocked_macs
27     return False
28
29 def save_blocked_mac(mac):
30     """Сохраняет MAC-адрес в файл заблокированных устройств."""
31     with open(BLOCKED_FILE, "a") as f:
32         f.write(mac + "\n")
33
34 def block_device(mac):
35     """Блокировка устройства по MAC-адресу через iptables и nftables."""
36     if is_already_blocked(mac):
37         bot.send_message(CHAT_ID, f"⚠️ Устройство с MAC {mac} уже заблокировано.")
38         return
39
40     # Блокировка через iptables
41     os.system(f"iptables -A INPUT -m mac --mac-source {mac} -j DROP")
42     os.system(f"iptables -A FORWARD -m mac --mac-source {mac} -j DROP")
43     os.system(f"iptables -A OUTPUT -m mac --mac-source {mac} -j DROP")
44
45     # Блокировка через nftables (если доступно)
46     os.system(f"nft add rule ip filter input ether saddr {mac} drop")
47
48     # Сохранение в файл
49     save_blocked_mac(mac)
50
51 # Логирование и сообщение
52 bot.send_message(CHAT_ID, f"🚫 Устройство с MAC {mac} заблокировано!")
53 log_event(f"Blocked device: {mac}")
54
55 def alert_admin(device):
56     """Отправляет уведомление о неизвестном устройстве и логирует событие."""
57     vendor = get_vendor(device['mac'])

```

Сурет 2. telegram_alert.py скрипты

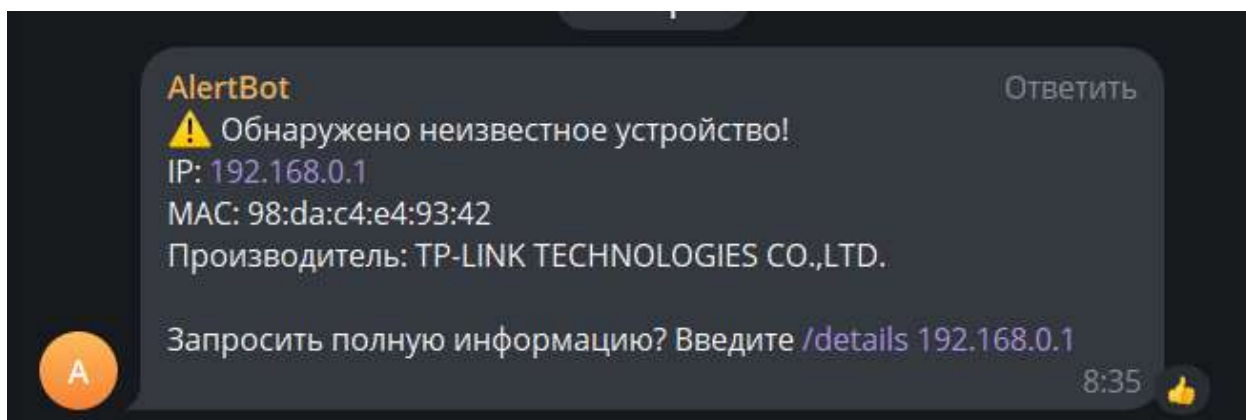
Бұл скрипт Wi-Fi желісіндегі белгісіз құрылғыларды автоматты түрде анықтап, Telegram арқылы әкімшіге хабарлама жібереді. Бағдарлама алдымен рұқсат етілген құрылғылардың тізімін (whitelist) жүктейді, содан кейін scan_network() функциясы арқылы желіні сканерлейді. Егер құрылғы whitelist тізімінде болмаса, оның MAC және IP мекенжайлары, өндірушісі туралы ақпаратпен бірге Telegram-ға хабарлама жіберіледі. Әкімші /details <IP> командасы арқылы қосымша ақпарат ала алады немесе /block <MAC> командасын қолданып, құрылғыны iptables және nftables арқылы бұғаттай алады. Сондай-ақ, /whitelist <MAC> командасы арқылы құрылғыны рұқсат етілгендер тізіміне қосуға болады, ал /network командасы желідегі барлық құрылғылардың тізімін көрсетеді. Бот блокталған құрылғылардың

тізімін blocked_devices.txt файлына сақтайды және барлық әрекеттерді network_alerts.log журналына жазады. Егер желіде бөтен құрылғылар табылмаса, бот Telegram-ға "В сети нет неизвестных устройств. Всё чисто." хабарламасын жібереді. Бағдарлама тұрақты жұмыс істеп, желіні үнемі бақылап отырады.

Список разрешенных MAC-адресов
1a:2b:3c:4d:5e:6f
7d:8e:9f:0a:1b:2c
9a:0b:1c:2d:3e:4f
5a:6b:7c:8d:9e:0f

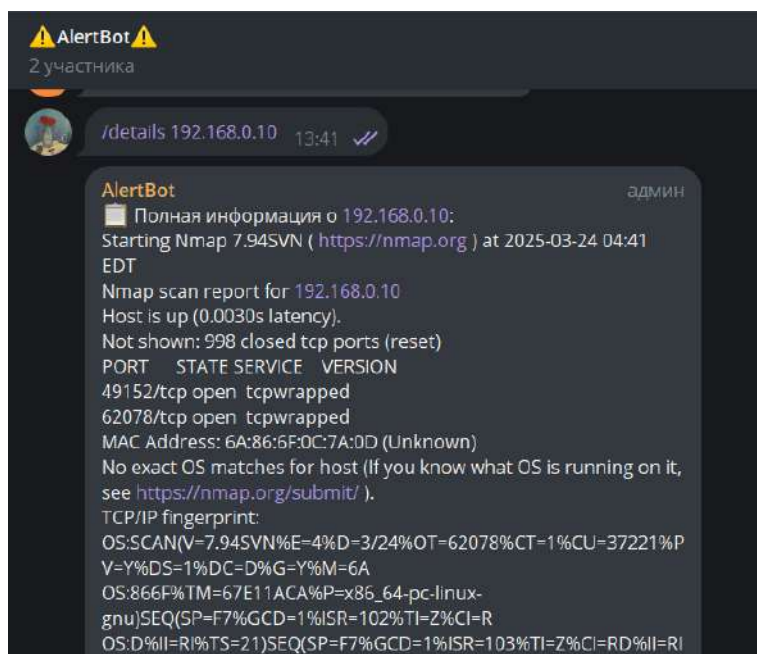
Рұқсат етілген MAC адресстер тізімі

Бұл бізде рұқсат етілген MAC адресстердің тізімі, яғни егер осы MAC адресстерден бөлек MAC адрес табылса телеграм арқылы уведомление келеді.



Сурет 3. Телеграмға келетін хабарлама түрі

AlertBot анықталмаған құрылғыны тапты және әкімшіге Telegram арқылы хабарлама жіберді. Хабарламада құрылғының IP-адресі (192.168.0.1), MAC-адресі (98:da:c4:e4:93:42) және өндірушісі (TP-LINK TECHNOLOGIES CO., LTD.) көрсетілген. Сонымен қатар, толық ақпарат алу үшін /details 192.168.0.1 командасын енгізу ұсынылады. Бұл жүйе желідегі бейтаныс құрылғыларды бақылауға және әкімшіге жылдам хабарлауға мүмкіндік береді.



Сурет 4. details командасы арқылы белгісіз құрылғы жайлы толық ақпарат алу

AlertBot толық ақпаратты ұсынды, ол 192.168.0.10 құрылғысына Nmap утилитасы арқылы сканерлеу жүргізді. Есепте құрылғының желіде белсенді екені (Host is up) және оның екі ашық порты бар екені (49152/tcp және 62078/tcp) көрсетілген. MAC-адресі 6A:86:6F:0C:7A:0D, бірақ өндірушісі анықталмаған. Операциялық жүйені нақты сәйкестендіру мүмкін болмады, бірақ TCP/IP fingerprinting нәтижелері көрсетілген. Traceroute нәтижесіне сәйкес, құрылғы желіде бір аралықтан кейін қолжетімді. Бұл ақпарат желі әкімшісіне құрылғының ашық порттарын және белсенділігін бақылауға көмектеседі.

Қорытынды. Бұл зерттеу жұмысы Wi-Fi желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесін әзірлеуге арналған. Қазіргі таңда ақпараттық қауіпсіздік маңызды мәселе болып табылады, және ұсынылған шешім желіге рұқсатсыз қосылған құрылғыларды анықтап, әкімшіге хабарлау арқылы қауіпсіздікті арттыруға бағытталған. Жүйе Python және Scapy кітапханаларының көмегімен жүзеге асырылып, ARP және DHCP сұраулары арқылы белсенді құрылғыларды анықтайды. Белгісіз құрылғылар сенімді құрылғылар тізімімен салыстырылып, сәйкессіздік анықталған жағдайда Telegram API арқылы әкімшіге хабарлама жіберіледі. Сонымен қатар, Kali Linux жүйесі негізінде жүргізілетін қауіпсіздік тесттері желінің қорғаныс деңгейін бағалауға мүмкіндік береді. Detect.py және Telegram_alert.py скрипттерінің үйлесімді жұмысы құрылғыларды анықтау, өндірушілерін талдау және қосымша желілік ақпарат алу процесін автоматтандырады. Егер белгісіз құрылғы анықталса, әкімші оның IP және MAC мекенжайлары, өндірушісі, ашық порттары және желідегі белсенділігі туралы толық мәлімет ала алады. Бұл жүйе ұйымдар мен жеке тұлғалар үшін киберқауіптерге қарсы қосымша қорғаныс қабатын қамтамасыз етеді. Сонымен қатар біздің әзірлеген қорғау жүйеміз шағын яғни көп шығынды, қымбат құрылғыларды қолдануға мүмкіндік болмаған wi-fi желілерінде де жұмыс жасайды. Осылайша, әзірленген жүйе Wi-Fi желілерін рұқсатсыз пайдаланудан қорғауға мүмкіндік береді және ақпараттық қауіпсіздікті нығайтуға бағытталған тиімді құрал болып табылады. Болашақта оның функционалын кеңейтіп, жасанды интеллект негізінде құрылғылардың мінез-құлқын талдау мүмкіндігін қосуға болады.

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]