

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

Подсекция 2.2

Интеллектуальные информационные системы

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

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

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

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

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

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «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. Рамагуллаев 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

қауіпсіздік қосымшаларына сенімділігін көрсете отырып, осыныларды растайды. Болашақта kuznychik өнімділігін оңтайландыру үшін гибриді іске асыруды немесе аппараттық жеделдетуді зерттеуге болады.

Қолданылған әдебиеттер тізімі

1. RFC 2144: The CAST-128 Encryption Algorithm // Internet Engineering Task Force (IETF). – 1997. – URL: <https://www.rfc-editor.org/rfc/rfc2144.txt>.
2. RFC 7801: GOST R 34.12-2015 Block Cipher "Kuznyechik" // Internet Engineering Task Force (IETF). – 2016. – URL: <https://www.rfc-editor.org/rfc/rfc7801.html>.
3. ISO/IEC 18033-3 Standard: Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers // International Organization for Standardization (ISO). – Geneva, 2005.
4. Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm // IOSR Journal of Engineering, Vol.6 Issue6, June 2016. – URL: [https://www.iosrjen.org/Papers/vol6_issue6%20\(part-1\)/A066010107.pdf](https://www.iosrjen.org/Papers/vol6_issue6%20(part-1)/A066010107.pdf) (дата обращения: 30.03.2025).
5. Profiling JVM Applications Remotely Using VisualVM // ITNEXT, June 2024. – URL: <https://itnext.io/profiling-jvm-applications-remotely-using-visualvm-c0df9816aabf> (дата обращения: 30.03.2025).

ӘӨЖ 004.056.5

ЖЕРГІЛІКТІ ЖЕЛІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТЕТІН НЕГІЗГІ ПАРАМЕТРЛЕР

Акимбекова Дильназ Маратовна, Каиржанова Дильназ Жалғасқызы

akimbekovadilnaz@mail.ru, dikairzhanova@gmail.com

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Қазіргі заманғы желілер кибершабуылдарға жиі ұшырайды, олардың ішінде рұқсатсыз қол жеткізу, «қызмет көрсетуден бас тарту» (DoS/DDoS) шабуылдары және деректерді ұстап қалу сияқты қауіптер бар. Желілік құрылғылардың қауіпсіздігін қамтамасыз ету ақпаратты қорғаудың және ықтимал шабуылдардың алдын алудың негізгі шараларының бірі болып табылады.

Үйлердегі немесе үй желілеріндегі жергілікті желілерге (LAN) ерекше назар аударған жөн. Үй желілері – бұл жергілікті желілердің бір түрі; олар интернетке қосылған құрылғылардың кең және алуан түрін қамтуы мүмкін және оларды басқару оңай, сенімді және қауіпсіз болуы керек, әсіресе олардың иелері көбінесе техникалық дағдылары жоқ пайдаланушылар болғандықтан [1].

Көптеген жылдар бұрын үй желісі сымсыз желіге қосылған бірнеше ноутбуктан тұрған. Бүгінгі таңда оған смартфондар, сымсыз принтерлер, термостаттар, дыбыс датчиктері, түтін датчиктері, шамдар, камералар, теледидарлар, аудио жүйелері, ақылды динамиктер, тоңазытқыштар және тағы басқалар кіруі мүмкін. "Заттар интернеті" (IoT, Internet of Things) деп аталатын интернетке үйлесімді құрылғылардың көбеюі кез-келген электрониканы, соның ішінде әртүрлі сенсорларды желіге қосуға мүмкіндік береді. Қосылған құрылғылардың бұл

үлкен ауқымы мен әртүрлілігі үй желілерін жобалауда, басқаруда және қорғауда жаңа қоңыраулар тудырады [1].

Желіге әртүрлі кибершабуылдар бағытталуы мүмкін. Ең алдымен, желілік шабуылдар туралы айтуға болады. ARP Spoofing немесе ARP Poisoning арқылы шабуылдаушы желідегі құрылғылардың MAC-адрестерін өзгертіп, өзін заңды құрылғы ретінде көрсетіп, трафикті ұстап қалуы мүмкін. DHCP Starvation шабуылы кезінде заңды пайдаланушыларға IP мекенжай тағайындалмайтындай етіп, шабуылдаушы DHCP серверін жалған сұраныстармен толтырады. Сондай-ақ, Man-in-the-Middle (MitM) шабуылы желідегі құрылғылардың байланысын бұзып, барлық деректерді өз арқылы өткізуге мүмкіндік береді.

Құрылғыларға бағытталған шабуылдардың ішінде брутфорс арқылы роутер, сервер немесе IoT құрылғыларының логині мен паролін күшпен тауып алу әдісі кең таралған. SSH немесе Telnet хаттамалары арқылы рұқсатсыз кіруге әрекет жасау да ықтимал қауіптердің бірі болып табылады. Бұған қоса, Denial of Service (DoS немесе DDoS) шабуылдары серверді немесе роутерді шамадан тыс сұраныстармен жүктеп, қызметін тоқтатуы мүмкін.

IoT құрылғылары да осалдықтарға ұшырауы мүмкін. Егер олардың әдепкі логині мен паролі өзгертілмеген болса, шабуылдаушылар оларды оңай анықтап, желіге еніп кетуі мүмкін. Сонымен қатар, IoT құрылғылардың бағдарламалық жасақтамасында осалдықтар болса, шабуылдаушы оларды өз мүддесіне пайдаланып, құрылғыны басқаруы мүмкін. Кейбір жағдайларда зиянды ботнеттер осындай IoT құрылғыларды жұқтырып, оларды үлкен масштабтағы DDoS шабуылдарына қолданады.

Ақпарат ұрлау және тыңшылық шабуылдары да үлкен қауіп төндіреді. Packet Sniffing әдісімен желі трафигін тыңдау арқылы шабуылдаушы құпия ақпаратты, парольдерді немесе жеке мәліметтерді ұрлай алады. DNS Spoofing шабуылында желі қолданушылары жалған веб-сайттарға бағытталып, олардың деректерін зиянды серверлерге жіберу мүмкін.

Сондай-ақ, физикалық шабуылдар да қауіпсіздікке елеулі әсер етеді. Мысалы, кабельді үзу немесе қайта қосу арқылы шабуылдаушы желіні бұзуы мүмкін. Желілік құрылғыларға рұқсатсыз физикалық қолжетімділік алу арқылы конфигурацияны өзгерту немесе жабдықты зақымдау да ықтимал.

Осындай шабуылдарды болдырмау үшін VLAN, ACL, брандмауэр, күшті аутентификация, шифрлау сияқты қорғаныс шараларын қолдану қажет. Желіні үнемі бақылап, осалдықтарды уақытында жою қауіпсіздікті арттыруға көмектеседі.

Бұл мақалада маршрутизаторлар, коммутаторлар және IoT құрылғылары сияқты желілік құрылғыларды қорғаудың негізгі әдістері қарастырылады, сонымен қатар олардың Packet Tracer-де модельдену мүмкіндіктері талданады.

Негізгі қорғаныс құралдарының бірі – маршрутизаторлардағы кіруді басқару тізімдерін (Access Control Lists, ACL) пайдалану. ACL сізге қажет емес қосылымдарды бұғаттау арқылы кіріс және шығыс трафикті сүзуге мүмкіндік береді. ACL пайдалану жергілікті желіге сырттан кіруді шектеуге және рұқсатсыз қосылу қаупін азайтуға көмектеседі. Олар екі түрге бөлінеді:

- Стандартты ACL - трафикті тек дереккөздің IP-мекен-жайы бойынша сүзеді.
- Жетілдірілген ACL - пакеттерді дереккөз бен алушының IP мекенжайы, порт нөмірі және протокол арқылы сүзуге болады.

Желіні виртуалды жергілікті желілерге (VLAN) бөлу шабуылдардың таралу аймағын азайтуға және желідегі жүктемені азайтуға мүмкіндік береді. Мысалы, IoT құрылғыларына бөлек VLAN бөлу негізгі желінің бұзылу қаупін азайтады.

VPN (Virtual Private Network) пайдалану интернет арқылы берілетін деректерді шифрлау арқылы қорғауға мүмкіндік береді. IPsec VPN кәсіпорын мен үй желілерін қорғау үшін қолданылады, дегенмен Cisco Packet Tracer толық функционалдығы жоқ тек негізгі VPN эмуляциясын қолдайды.

IoT құрылғылары көбінесе әлсіз кірістірілген қорғанысқа ие, сондықтан оларды бөлек VLAN-ға орналастыру керек. Бұл құрылғылардың негізгі желімен өзара әрекеттесуін шектейді және олардың бұзылу қаупін азайтады. IoT құрылғыларының Интернетке қол жетімділігін шектеу үшін ACL пайдалану олардың осалдығын азайтуға мүмкіндік береді.

IoT құрылғыларының микробағдарламасын үнемі жаңартып отыру осалдықтарды жоюға мүмкіндік береді. Packet Tracer ішіндегі микробағдарламаны жаңарту эмуляцияланбайды, бірақ оны веб-интерфейс немесе SSH арқылы қолмен жасау керек. Secure Shell (SSH) - бұл салыстырмалы түрде қарапайым және арзан болатындай етіп жасалған қауіпсіз желілік байланыс протоколы [2].

IoT құрылғылары желінің әлсіз нүктесі болғандықтан, сондықтан олар үшін қосымша қорғаныс шаралары қабылданды. Жеке VLAN және оқшаулау: IoT құрылғылары бір-бірімен байланыса алады, бірақ негізгі желіге қосыла алмайды. IoT VLAN-ынан интернетке тікелей шығу шектелді. ACL арқылы: IoT құрылғылары тек басқару серверімен байланыса алады. Администратор ноутбугі ғана IoT құрылғыларын басқара алады. Қауіпсіздік саясаты: Желідегі барлық IoT құрылғылары статикалық IP мекенжайлармен конфигурацияланды. Белгісіз MAC мекенжайлары бар құрылғыларға желіге қосылуға тыйым салынды.

Күрделі құпия сөздерді және екі факторлы аутентификацияны (2FA) пайдалану желілік жабдықтың қауіпсіздігін арттырады. Деректердің жоғалуын және желінің тоқтап қалуын болдырмау үшін келесі шаралар қолданылды. Резервтік көшірме жасау: Желі құрылғыларының конфигурациясы тұрақты түрде сақталады. Маңызды деректерді сақтау үшін серверге қол жеткізу шектелді. Қауіпсіз қашықтықтан басқару: Барлық әкімшілік әрекеттер тек SSH арқылы жүзеге асырылады. Барлық пайдаланушылар үшін күшті пароль саясаты енгізілді.

Желілік құрылғылардың қауіпсіздігін қамтамасыз ету үшін бірқатар шаралар қабылданды:

Брандмауэр (ACL) маршрутизаторда: Қауіпсіздік ережелері арқылы рұқсат етілмеген трафикті бұғаттау. Әкімшіге (Admin) тек өз құрылғысынан SSH арқылы маршрутизаторға қосылуға рұқсат беру. және IoT құрылғылары мен серверге тек белгілі IP мекенжайларынан ғана қосылуға мүмкіндік беру арқылы жалпы қауіпсіздікті қамтамасыз етеміз.

Желі сегментациясы (VLAN): Негізгі құрылғыларды (ноутбук, сервер, компьютер) жеке VLAN-ға орналастыру. IoT құрылғыларын бөлек VLAN-да оқшаулау, олардың ішкі желіге қолжетімділігі шектелді.

Портқа негізделген VLAN артықшылықтары:

- Орнатудың қарапайымдылығы. Ethernet порттарын топтастыру негізінде виртуалды желілерді құру көп жұмысты қажет етпейді, белгілі бір VLAN-ға кіретін әрбір Ethernet портына бірдей VLAN идентификаторын тағайындау жеткілікті.

- Хосттардың физикалық қозғалысынсыз желінің логикалық топологиясын өзгерту мүмкіндігі. Ethernet портының параметрлерін осы порттың параметрлерінде басқа VLAN идентификаторын көрсету арқылы өзгерту жеткілікті (мысалы, техникалық бөлімнің VLAN идентификаторын сату бөлімінің VLAN идентификаторына өзгерту) және жұмыс станциясы бірден жаңа VLAN ресурстарын пайдалануға мүмкіндік алады [3].

Қауіпсіз қашықтан басқару: Telnet-ті өшіріп, тек SSH арқылы маршрутизатор мен коммутаторларға қосылу қамтамасыз етілді. Күшті парольдер енгізу және барлық басқару интерфейстеріне рұқсатты шектеу.

Коммутаторлардағы MAC мекенжайларын сүзу рұқсат етілмеген құрылғыларды блоктауға мүмкіндік береді. Желіде қолданушылар мен құрылғылардың рұқсатсыз әрекеттерін болдырмау үшін келесі шаралар енгізілді: MAC-мекенжайлар бойынша бақылау (Port Security). Әрбір портқа белгілі бір MAC-мекенжайлар ғана қосыла алады. Бөгде құрылғы қосылған жағдайда порт автоматты түрде бұғатталады. Жеке интерфейстерден басқа, MAC-адрес интерфейстер тобын немесе тіпті барлық желілік интерфейстерді анықтай алады [4].

Қол жеткізуді бөлу: Администратор (ноутбук) - маршрутизатор, коммутатор және серверге толық қолжетімділікке ие. Кәдімгі пайдаланушылар (PC, Laptop) - серверге тек HTTP/HTTPS арқылы қосыла алады. IoT құрылғылары - тек өз VLAN ішінде байланыса алады, негізгі желіге кіре алмайды. Жүйелік оқиғаларды бақылау: Барлық маңызды оқиғалар syslog-серверге тіркеледі. SSH арқылы әрбір кіру әрекеті журналға жазылады.

Операциялық жүйеде, құрылғыда немесе қолданбада орын алатын оқиғаларды журналдау - ақпараттық қауіпсіздікті қамтамасыз ету процесінің ажырамас бөлігі. Қауіпсіздік журналдарындағы оқиғалардың болуына қарай желіге шабуыл жасау әрекетін алдын ала анықтауға болады. Егер оқиға орын алса, журналдағы жазбалар оны тергеуге көмектесе алады. Сондықтан қолданбалы деңгейдегі Syslog хаттамасы ақаусыз жұмыс істеуі керек. Ірі желілерде оқиғаларды жинау үшін әдетте барлық құрылғылар мен қолданбалардан оқиғаларды алатын орталық Syslog сервері қолданылады. Хакер белгілі бір құрылғыны бұзуға тырысады. Егер ол сәтті болса, онда құрылғыдағы оқиғалар журналын тазалай алады. Алайда бұл оқиғалар туралы жазбалар орталық Syslog серверінде сақталады [5].

Әрекетті бақылау үшін желі оқиғаларын түсіретін syslog серверін конфигурациялауға болады.

ACL пайдалану күдікті трафикті блоктауға көмектеседі, бірақ жетілдірілген талдау үшін Snort сияқты интрузияны анықтау жүйелерін (IDS) қолданған дұрыс. Алайда, Packet Tracer IDS-ке қолдау көрсетілмейді.

Журналдар арқылы хабарландыруларды эмуляциялау қауіпті анықтауды автоматтандыруға мүмкіндік береді. Желідегі кез келген күдікті әрекеттерді ерте анықтау үшін бақылау шаралары енгізілді. Желілік трафикті бақылау: Packet Tracer Simulation Mode арқылы нақты уақытта трафикті талдау. Қауіпті немесе рұқсат етілмеген трафикті автоматты түрде бұғаттау үшін ACL ережелері енгізілді. Желі құрылғыларының жұмысына мониторинг: SNMP көмегімен құрылғылардың жұмысын бақылау. Syslog сервері арқылы қауіпсіздік оқиғаларын жинау.

Практикалық жұмыстың нәтижесінде біз осындай қорытындыға келеміз:

Ақпараттық қауіпсіздікті қамтамасыз ету мақсатында желіде қатаң қолжетімділік саясаты енгізілді. Бұл саясат құрылғылар арасындағы өзара әрекеттестікті реттеп, маңызды желілік түйіндерге рұқсатты пайдаланушылардың рөлі мен құрылғылардың функционалдық мүмкіндіктеріне сәйкес шектейді.

Әкімші қолжетімділігі:

Желіні басқару және бақылау үшін әкімшінің ноутбугіне кеңейтілген рұқсаттар берілген. Әкімші маршрутизаторға SSH протоколы арқылы қосыла алады, бұл оған желіні қашықтан басқаруға мүмкіндік береді. Сонымен қатар, әкімші коммутаторға SSH және SNMP арқылы қосылып, оның параметрлерін өзгерте алады және желілік трафикті бақылай алады.

Серверге әкімші тек басқару мақсатында қосыла алады. Бұл қосылу SSH және HTTP арқылы жүзеге асырылады, ал басқа хаттамаларға шектеу қойылған. IoT құрылғыларына әкімшінің қолжетімділігі жоқ, себебі олар басқа VLAN-да оқшауланған.

Қауіпсіздік шаралары ретінде SSH қолданылады, бұл деректердің шифрланған байланысын қамтамасыз етеді және Telnet-ке қарағанда анағұрлым қауіпсіз болып табылады. Желілік құрылғыларға кіру парольмен қорғалған, ал SNMP қызметі тек әкімшіге рұқсат етілген.

Пайдаланушылардың қолжетімділігі:

Кәдімгі пайдаланушылардың желіге қосылу мүмкіндігі шектеулі. Олар серверге HTTP протоколы арқылы қосылып, ондағы қызметтерді пайдалана алады.

Маршрутизаторға, коммутаторға және IoT құрылғыларына пайдаланушылардың қолжетімділігі жоқ. Бұл желінің тұрақтылығын қамтамасыз ету және пайдаланушылардың маңызды желілік құрылғыларға әсер ету мүмкіндігін болдырмау үшін жасалған.

Қауіпсіздік мақсатында пайдаланушылардың желілік құрылғыларға SSH арқылы қосылу әрекеттері бұғатталған. Серверге қосылу тек HTTP арқылы жүзеге асырылады, ал SSH қолжетімді емес. Сонымен қатар, коммутаторда MAC-мекенжай бойынша бақылау механизмі енгізілген, бұл рұқсат етілмеген құрылғылардың желіге қосылуын шектейді.

Серверге қолжетімділік:

Сервер әкімші мен пайдаланушылардың сұраныстарын өңдейді. Пайдаланушылар HTTP арқылы сұраныстар жібере алады, ал әкімші тек SSH арқылы қосыла алады. IoT құрылғыларының сервермен байланысы шектелген, бұл ACL (Access Control List) көмегімен жүзеге асырылады.

Сервердің қауіпсіздігін қамтамасыз ету үшін тек қажетті порттар ашық. HTTP және SSH порттарынан басқа барлық кіріс трафигі бұғатталған. ACL ережелері IoT құрылғыларынан серверге келетін сұраныстарды қабылдамайды, осылайша ықтимал қауіптерді азайтады. Сонымен қатар, сервер конфигурациясының резервтік көшірмесі жасалады, бұл істен шыққан жағдайда жүйені қалпына келтіруді жеңілдетеді.

IoT құрылғыларының қолжетімділігі:

IoT құрылғылары оқшауланған VLAN ішінде орналасқан және олардың желіге қосылу мүмкіндіктері шектелген. Олар тек Home Gateway арқылы байланыс орнатуға рұқсат етілген. Мысалы, бейнебақылау камерасы тек белгілі IP-мекенжайларға бейне ағын жібере алады, ал басқа құрылғылармен өзара әрекеттесе алмайды.

IoT құрылғыларына интернетке шығуға тыйым салынған. Сонымен қатар, олар сервермен немесе басқа VLAN-дармен байланыса алмайды. Бұл олардың ықтимал шабуыл нысаны болуын болдырмау үшін маңызды шара болып табылады.

Қауіпсіздік шаралары ретінде ACL арқылы шектеулі қолжетімділік орнатылды. IoT құрылғылары жеке VLAN ішінде оқшауланған, бұл олардың басқа желілерге кіру мүмкіндігін шектейді. Сонымен қатар, сыртқы құрылғылардың IoT желісіне кіруіне толық тыйым салынған.

Қолданылған әдебиеттер тізімі

1. Andrew S. T., Nick F., David W. Computer Networks // Pearson Education Limited. – 2021. – ISBN 978-1-292-37406-2. - С. 18-20.
2. Столлинс У. Network Security Essentials: Applications and Standards // Prentice Hall. – 2011. – ISBN 978-0-13-610805-4. - С. 162.
3. Лапони́на О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны // Национальный Открытый Университет «ИНТУИТ». - 2014. - С. 41.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. 2-е изд. // Учебник для вузов. - С. 419.
5. Бирюков А.А. Информационная безопасность: защита и нападение // ДМК Пресс. – 2023. – №3. – С. 138.

УДК 004

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДА И ИНСТРУМЕНТА ДЛЯ ВЫЯВЛЕНИЯ ФЕЙКОВЫХ НОВОСТЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Аскарлов Абылай Дарханулы
askarovabylay@yandex.kz