

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 Жасиинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған 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. 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

2. Инциденты информационной безопасности: выявление, расследование и реагирование // <https://selectel.ru/blog/security-incidents/> (дата обращения: 23.03.2025)
3. Что такое SIEM ? // <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem> (дата обращения: 25.03.2025)
4. План реагирования на инциденты кибербезопасности: что это и почему он нужен каждой организации // <https://ddos-guard.ru/blog/plan-reagirovaniya-na-incidenty-kiberbezopasnosti> (дата обращения: 25.03.2025)
5. Отакулов Артур Собинович Способы реагирования на инциденты информационной безопасности // E-Scio. 2020. №1 (40). URL: <https://cyberleninka.ru/article/n/sposoby-reagirovaniya-na-intsidenty-informatsionnoy-bezopasnosti> (дата обращения: 31.03.2025).
6. Русскевич Евгений Александрович Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. №11 (96). URL: <https://cyberleninka.ru/article/n/ponyatie-vredonosnoy-kompyuternoy-programmy> (дата обращения: 31.03.2025).
7. Голубятников Артем Олегович DDOS-АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ // E-Scio. 2022. №10 (73). URL: <https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi> (дата обращения: 31.03.2025).
8. Что такое социальная инженерия ? // <https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering> (дата обращения: 31.03.2025)

УДК 004.056

MITM ШАБУЫЛЫ (АДАМНЫҢ ОРТАДАҒЫ ШАБУЫЛЫ)

Қартбай Елнұр Ғалымжанұлы
Тынарбай Назым Исламбекқызы

shattik59@gmail.com, tynarbayn@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті
Ақпараттық қауіпсіздік жүйелері кафедрасының студенттері, Астана, Қазақстан
Ғылыми жетекші: Казиева Назым Магидулловна

Аңдатпа

Бұл мақалада Man-in-the-Middle (MITM) шабуылының негізгі түрлері, орындалу механизмдері және олардың қауіпсіздікке тигізетін ықпалы қарастырылған. MITM шабуылы желідегі деректер алмасуға араласу арқылы ақпаратты ұрлау немесе өзгертуге мүмкіндік береді. MITM шабуылын жүзеге асыру үшін ARP-spoofing, DNS-spoofing, SSL-stripping сияқты әдістер кеңінен қолданылады. Бұл зерттеу аясында Kali Linux жүйесінде Bettercap құралы арқылы ARP-spoofing шабуылының орындалу тәсілдері зерттеліп, трафикті ұстап алу және өзгерту процесі көрсетілген. Сонымен қатар, MITM шабуылынан қорғану жолдары, HTTPS, VPN, ARP-қорғаныс механизмдері және жүйелік қауіпсіздік шаралары талданды. Бұл зерттеу MITM шабуылдарының механизмдерін тереңірек зерттеу негізінде желілік қауіпсіздікті күшейту бағыттары анықталған.

Кілт сөздер: MITM шабуылы, ARP-spoofing, Kali Linux жүйе, Better Cap құралы, желілік қауіпсіздік.

Кіріспе. Қазіргі таңда ақпараттық қауіпсіздік кибершабуылдардың қарқынды дамуына байланысты маңызды мәселелер туындалуда. Ақпараттық технологиялардың дамуы "Man-in-the-Middle" (MITM) шабуылының жиі орын алуына ықпал етеді. Бұл шабуыл кезінде қаскүнем

екі тарап арасындағы деректердің алмасуына араласып, ақпараттар ұрлануға немесе оны өзгертуге мүмкіндіктер алады. MITM шабуылы қаржы ұйымдарына, мемлекеттік мекемелерге, жеке кәсіпорындарға, тіпті қарапайым пайдаланушыларға да қауіп төндіреді [1, 2].

MITM шабуылдары көбінесе ашық және осал Wi-Fi желілерінде, шифрланбаған трафиктерде және әлсіз қорғаныс жүйелері бар желілік инфрақұрылымдарда орын алады. Қаскүнемдер ARP-spoofing, DNS-spoofing, SSL-stripping және басқа да әдістерді қолдану арқылы өз жәберіленуші желілік трафиктерін бақылап, қол жеткізе алады.

Бұл зерттеу жұмысында MITM шабуылының негізгі түрлері, олардың орындалу механизмдері және қауіпсіздікке тигізетін әсері талданды. Сондай-ақ, Kali Linux операциялық жүйесінде Bettercap құралын пайдалану арқылы ARP-spoofing шабуылының орындалу әдістері зерттеліп, шабуылдың орындалу кезеңдері мен қорғану әдістері қарастырылды.

Зерттеудің мақсаты - MITM шабуылдарының қауіптілігін көрсету, олардың орындалу әдістерін сипаттау және қорғаныс шараларын ұсыну.

Зерттеу әдістері. Зерттеу барысында жалпы ғылыми және арнайы таным, оның ішінде жүйелік талдау және синтез, теориялық жалпылау әдістері қолданылды.

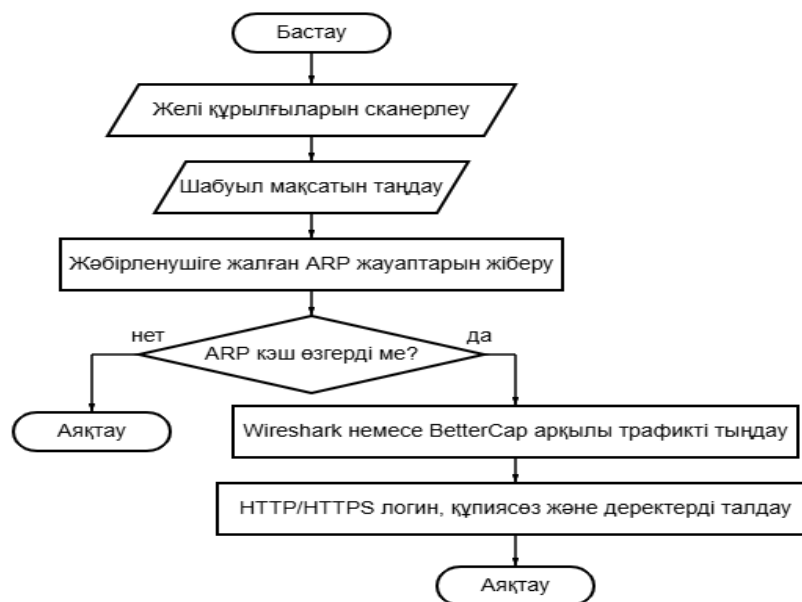
Талқылау және нәтижелер. Зиянкестер, шабуылдаушылар интернет-байланысын бақылау үшін әртүрлі тәсілдерді қоладанады [2]. Бұл әдістердің барлығы пайдаланушылардың деректерін ұрлауға, фишингтік шабуылдар жасауға, бұдан басқа жүйелерге кіруге мүмкіндік береді.

Қолданылатын әдістерге қарамастан, ортадағы адам шабуылдарының көпшілігі қарапайым әрекеттер тізбегін бақылайды. Мысалы: Алиса, Боб және Чак (шабуылдаушы) [3].

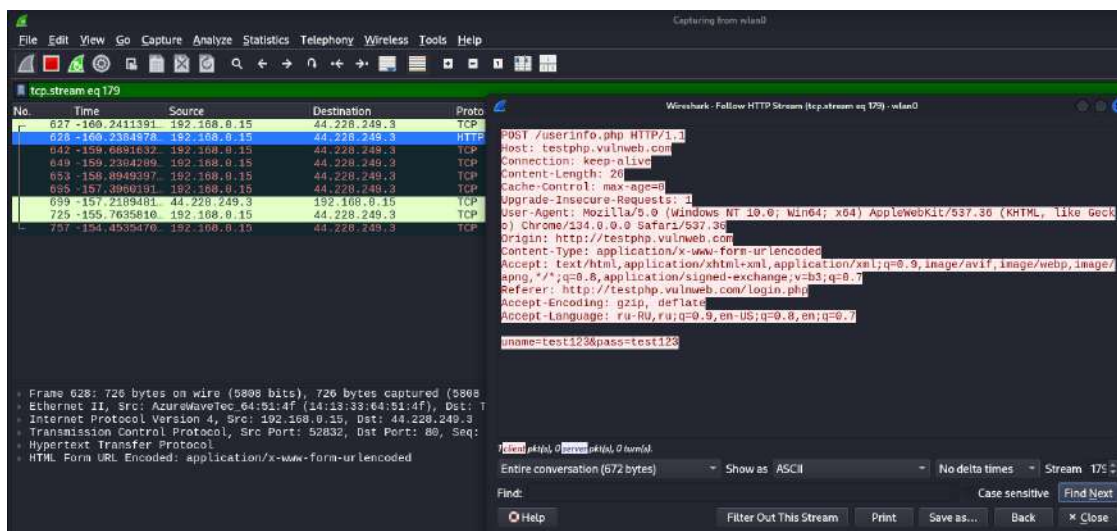
1. Чак Элис пен Бобтың байланысын тыңдайды.
2. Алиса Бобқа хабарлама жібереді.
3. Чак оны ұстап алып оқиды.
4. Чак хабарды өзгертіп, Бобқа жібереді.

«Ортадағы адам» (MITM) шабуылдары көбіне кибершабуылдың бастапқы кезеңдерінде қолданылады, яғни барлау, жүйеге кіру және зиянды әрекеттерді орындайды. Бұл әдіс арқылы шабуылдаушылар пайдаланушы мәліметтерін ұстап қалып, желідегі әрекеттерді бақылай алады.

MITM шабуылы желілік трафикті ұстап, оны өзгертуге немесе тыңдауға мүмкіндік беретін қауіпті кибершабуылдардың бірі болып табылады. Бұл шабуылдың ең көп таралған түрлерінің бірі - ARP Spoofing. Бұл әдіс жергілікті желіде орындалады және шабуылдаушыға трафикті өз құрылғысы арқылы өткізуге мүмкіндік береді (Сурет 1).



Сурет 1. "ARP Spoofing алгоритмі"



Сурет 2. Wireshark арқылы трафикті ұстап алу

Сурет 2. `arp spoof -i eth0 -t 192.168.0.15 192.168.0.1` командасын қолдану арқылы желілік трафикті ұстап алу және шабуыл жасау процестері сипатталған.

Bettercap - желілік трафикті талдауға, ARP спуфинг жасауға, Man-in-the-Middle (MITM) шабуылдарын орындауға арналған қуатты құрал (Сурет 3). Төменде көрсетілген әрекеттер Kali Linux-та Bettercap көмегімен жүзеге асырылған желілік шабуылды сипаттайды.

1. `bettercap -iface wlan0` команда арқылы WLAN интерфейсінде Bettercap қосылып, желіні бақылауға дайындық жасайды.

2. `net.probe on` команда желідегі барлық белсенді құрылғыларды анықтап, олардың IP, MAC және өндіруші (Vendor) ақпаратын жинау мүмкіндіктеріне ие.

3. *arp.spoof on* әрекет шабуылдаушыға өзін желілік шлюз ретінде көрсетуге мүмкіндік алады, маршрутизатор ARP спуфингтен қорғалмаған болса, шабуыл сәтті орындалып, толық дуплексті (full-duplex) трафик бағытын өзгерту мүмкіндігіне ие болады.

```
(yelnur@nazym)~$ sudo bettercap -iface wlan0
[sudo] password for yelnur:
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.16 » [21:45:50] [sys.log] [inf] gateway monitor started ...
192.168.0.0/24 > 192.168.0.16 » net.probe on
[21:46:53] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[21:46:53] [endpoint.new] endpoint 192.168.0.15 detected as 14:13:33:64:51:4f (AzureWave Technology Inc.).
192.168.0.0/24 > 192.168.0.16 » [21:46:53] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24
[21:46:53] [endpoint.new] endpoint 192.168.0.11 detected as de:73:2f:45:2c:5d.
192.168.0.0/24 > 192.168.0.16 » [21:46:53] [endpoint.new] endpoint 192.168.0.12 detected as de:51:eb:82:2b:6a.
192.168.0.0/24 > 192.168.0.16 » [21:47:01] [endpoint.new] endpoint 192.168.0.10 detected as d6:ec:d5:36:68:6d.
192.168.0.0/24 > 192.168.0.16 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.16	a8:42:a1:b0:eb:40	wlan0	TP-Link Corporation Limited	0 B	0 B	21:45:50
192.168.0.1	20:98:d8:13:29:ee	gateway	Shenzhen Yingdakang Technology CO., LTD	4.1 kB	1.9 kB	21:45:50
192.168.0.10	d6:ec:d5:36:68:6d			0 B	92 B	21:47:01
192.168.0.11	de:73:2f:45:2c:5d			140 B	184 B	21:47:01
192.168.0.12	de:51:eb:82:2b:6a			264 B	184 B	21:47:01
192.168.0.15	14:13:33:64:51:4f	DESKTOP-TEF9IQ9	AzureWave Technology Inc.	519 B	787 B	21:47:01

Сурет 3. Bettercap құралы арқылы желілік шабуыл

Ал Bettercap желі арқылы өтетін барлық трафикті тыңдап, оны талдауға кіріседі. Бұл әрекет барысында DNS сұраныстары мен жауаптары, HTTP трафигі, оның ішінде POST сұраныстары, логин мен пароль туралы мәліметтер ұсталып қалады (Сурет 4).

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Connection: keep-alive
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Content-Length: 26
Cache-Control: max-age=0
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate

uname=test123&pass=test123

192.168.0.0/24 > 192.168.0.16 » [21:56:37] [net.sniff.http.request] http: DESKTOP-TEF9IQ9 POST testphp.vulnweb.com/userinfo.php
```

Сурет 4. Желі трафигін тыңдау (Sniffing)

Осылайша, шабуылдаушы ARP спуфинг және трафикті тыңдау әдістерін қолдана отырып, қорғалмаған HTTP аутентификациялық мәліметтерін оңай ұстап ала алады. Мұндай қауіптердің алдын алу үшін HTTPS пайдалану, ARP қорғау механизмдерін қосу және желідегі күдікті әрекеттерді бақылау үшін маңызды.

ARP спуфинг шабуылын орындау үшін бұл зерттеуде екі түрлі әдіс қолданылды: **Arpspoof** және **Bettercap** құралы. 1-кестеде осы әдістердің мүмкіндіктері салыстырмалы түрде көрсетілген [6].

Кесте 1. Arpspoof және Bettercap құралдары

Критерий	Arpspooф	Bettercap
Қолдану қарапайымдылығы	Қолдану үшін бірнеше команданы қолмен орындау қажет, сондай-ақ шабуылдың нысанын нақты көрсету талап етіледі.	Bettercap интерактивті интерфейсі бар, қолдануға ыңғайлы әрі қосымша функционалдары жеткілікті.
Желі құрылғыларын анықтау	Қолмен енгізілген IP мекенжайына ғана шабуыл жасайды, яғни автоматты түрде құрылғыларды анықтау мүмкіндігі жоқ, шабуылды дайындау уақыты ұзағырақ.	net.probe on командасын орындау арқылы желідегі барлық белсенді құрылғыларды автоматты түрде анықтап, жылдам шабуыл жасай алады.
Функционалдық мүмкіндіктер	Бұл құрал тек ARP спуфинг шабуылын іске асырып, трафикті қайта бағыттау үшін қолданылады.	Bettercap тек ARP спуфингпен шектелмейді, ол сонымен қатар DNS Spoofing, Sniffing және Man-in-the-Middle (MITM) шабуылдарын жүзеге асыра алады.
Трафикті бақылау (Sniffing)	Желідегі деректерді тыңдау үшін қосымша бағдарламалар (мысалы, Wireshark) қажет.	Bettercap өз ішінде трафикті ұстап, оны талдауға мүмкіндік береді.
Жасырындық деңгейі	Бұл әдіс қосымша құралдарды қажет ететіндіктен, шабуылды анықтау ықтималдығы жоғары.	Барлық процестерді орталықтандырылған түрде басқаруға мүмкіндік береді, бұл шабуылды тиімді орындауға және жасырын әрекет етуге көмектеседі.
Қорғану механизмдерінен айналып өту	Қарапайым шабуылдарды орындауға мүмкіндік береді, бірақ қорғанысы жоғары желілерге шабуылдау қиынырақ.	Бұл құрал динамикалық шабуылдарды орындауға, әртүрлі MITM әдістерін біріктіруге және қорғаныс механизмдерін айналып өтуге мүмкіндік береді.

Зерттеу барысында ARP спуфинг шабуылынан қорғану мақсатында ARP Saqshy бағдарламасы құрастырылды, бағдарлама шабуылды анықтайды және алдын алатын графикалық қосымшаны жасайды.

ARP Spoofing қорғаныс бағдарламасы және оның коды [7]

Біздің қарастырған қорғаныс құрылғысы қалай жұмыс істейді?

1. Желі туралы ақпаратты алады – роутердің IP және MAC-адресін анықтайды.
2. ARP-кәшті тексереді – роутердің MAC-адресі өзгергенін бақылайды.
3. Жаңартылған MAC-адреспен салыстырады – егер өзгеріс байқалса, шабуыл туралы ескертеді.
4. Ескерту береді – дыбыстық сигнал, экрандық хабарлама және жұмыс үстелі арқылы.
5. Желіні өшіреді – қауіп анықталса, интернет автоматты түрде өшіріледі.
6. ARP-кәшті тазалайды – қажет болғанда желіні қорғау үшін.
7. ARP-кестесін көрсетеді – arp -а командасына ұқсас желідегі құрылғылардың IP және MAC-адрестерін шығарады.

Ортадағы адам (MITM) шабуылдары желідегі осалдықтарды пайдаланып, пайдаланушылардың құпия мәліметтерін ұрлауға бағытталады. Мұндай шабуылдардан қорғану үшін киберқауіпсіздік шараларын сақтау өте маңызды.

Қорытынды. Ең алдымен, **қауіпсіз желіге қосылу** басты шарт болып табылады. Белгісіз немесе ашық Wi-Fi желілеріне қосылу үлкен қауіп төндіреді, сондықтан WPA2/WPA3 қорғанысы бар маршрутизаторларды қолдану керек. Сонымен қатар, **VPN қызметін пайдалану** желідегі трафикті шифрлап, оны үшінші тараптардың бақылауынан қорғайды. **Желідегі мәліметтерді шифрлау** да маңызды рөл атқарады. HTTPS қосылымдарын ғана пайдалану, электрондық пошта мен хабарламаларды түпкілікті шифрлауды қосу ақпараттың қауіпсіздігін арттырады. **DNS сұрауларын шифрлау** арқылы DNS-спуфинг сияқты шабуылдардың алдын алуға болады.

Қауіпсіздікті күшейтудің тағы бір маңызды аспектісі - **жүйелік жаңартуларды уақытылы орнату және антивирус пен брандмауэрді белсенді ұстау**. Бұл зиянды бағдарламалар мен шабуылдарды ерте анықтауға көмектеседі.

Бұдан бөлек, **құпиясөздерді қауіпсіз сақтау және қайта пайдаланбау** үшін құпиясөз менеджерін қолдану қажет. **Көп факторлы аутентификацияны (MFA) енгізу** есептік жазбалардың қосымша қорғалуын қамтамасыз етеді. Желілік қауіпсіздікті арттыру үшін **нөлдік сенім принципін (Zero Trust)** қолдану қажет, яғни жүйеге кірген пайдаланушылар мен құрылғыларға автоматты түрде сенім білдірудің орнына, әрбір кіру әрекеті мұқият тексерілуі тиіс. Сонымен қатар, **желілік белсенділікті бақылау** арқылы күдікті әрекеттерді ерте анықтап, шабуылдардың алдын алуға болады.

Жалпы, жоғарыда аталған әдістерді қолдану желілік қауіпсіздікті күшейтіп, MitM шабуылдарынан тиімді қорғануға мүмкіндік береді. Киберқауіпсіздік - бұл бір реттік емес, үздіксіз процесс, сондықтан әрбір пайдаланушы өзінің жеке деректерін қорғауға жауапкершілікпен қарауы қажет.

Пайдаланылған әдебиеттердің тізімі

1. John Martinez. Man-in-the-Middle (MITM) Attack: Definition, Examples & More: <https://www.strongdm.com/blog/man-in-the-middle-attack> 03.01.2025 (Время посещения 20.03.2025)
2. Man-in-the-middle attack: <https://encyclopedia.kaspersky.com/glossary/man-in-the-middle-attack/> (Время посещения 21.03.2025)
3. Jeff Petters. Man-in-the-Middle: советы по обнаружению и предотвращению: <https://habr.com/ru/companies/varonis/articles/526632> 05.11.2020 (Время посещения 20.03.2025)
4. ARP Мағынасы Kazakh: <https://goong.com/kk/word/arp-мағынасы--kazakh/> (Время посещения 22.03.2025)
5. Защита от MITM атак: Примеры инструменты и советы: <https://sky.pro/wiki/javascript/zashita-ot-mitm-atak-primery-instrumenty-i-sovety/> (Время посещения 25.03.2025)
6. ARP Spoofing: <https://www.prosec-networks.com/en/blog/arp-spoofing/> (Время посещения 29.03.2025)
7. Kartbay Yelnur & Tynarbay Nazym. ARP Saqshy: <https://github.com/Elikon0106/ARP-Saqshy/tree/main> (Время создания 28.03.2025)

ӘОЖ 004.056

**ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ ҚАУІПСІЗДІККЕ ҚАТЕР РЕТІНДЕ:
ҚЫЗМЕТКЕРЛЕРДІ ҚОРҒАУ ЖӘНЕ ОҚЫТУ ӘДІСТЕРІ**