

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

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

**Студенттер мен жас ғалымдардың  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»  
XIX Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XX Международной научной конференции  
студентов и молодых ученых  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS  
of the XX International Scientific Conference  
for students and young scholars  
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 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 «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
<b>Подсекция 2.4</b>		
<b>Информационная безопасность</b>		
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

күйінде берілуі жүйенің осалдығын арттырады. Бұл MITM (Man-in-the-Middle) шабуылдары мен деректердің ұрлану қаупін тудырады.

Желілік қауіпсіздікті арттыру үшін шифрлау механизмдерін күшейту, аутентификацияны жетілдіру және желілік трафикті үнемі бақылау қажет. TLS 1.3 және Perfect Forward Secrecy технологияларын қолдану деректердің қауіпсіздігін қамтамасыз етеді. Сонымен қатар, HTTP Strict Transport Security механизмі арқылы MITM шабуылдарының алдын алуға болады. Құпиясөздерді серверге жібермес бұрын хештеу және қосымша аутентификация әдістерін енгізу пайдаланушы деректерін қорғаудың тиімді әдістері болып табылады.

Жалпы, Wireshark сияқты құралдарды тиімді пайдалану ұйымдардың ақпараттық қауіпсіздігін нығайтуға және ықтимал киберқауіптерден қорғануға мүмкіндік береді. Дұрыс конфигурацияланған желілік қауіпсіздік жүйесі шабуылдардың алдын алуға және маңызды деректерді қорғауға көмектеседі.

### **Қолданылған әдебиеттер тізімі**

1. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
2. Bejtlich, R. (2004). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley.
3. Sanders, C. (2017). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). No Starch Press.
4. Orebaugh, A., Ramirez, G., Beale, J., Burke, J., & Wright, L. (2006). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress.
5. Scarfone, K., & Mell, P. (2009). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology (NIST).
6. Chappell, L. (2017). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide* (2nd ed.). Protocol Analysis Institute.
7. Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

### **MITM ШАБУЫЛЫ ТУРАЛЫ**

#### **Кәкімбек Әділ Қайроллаұлы, Серікбай Ақжол Ерболатұлы, Наурызбаев Дарын Ерболатұлы**

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің ақпараттық қауіпсіздік жүйелерінің оқытушысы, Астана, Қазақстан  
Ғылыми жетекшісі – Н.Казиева

Ортадағы адам (MITM) шабуылы – шабуылдаушы тікелей байланысып жатыр деп есептейтін екі тарап арасындағы байланысты ұстап алатын және ықтимал өзгертетін кибершабуыл түрі.[3] MITM шабуылдарының табиғатын, оларды анықтау және алдын алу әдістерін және нақты әлемде қолдану жағдайларын тереңірек түсіну үшін келесі мақалаларды оқуды ұсынамыз: «Ортадағы адам: анықтау және алдын алу бойынша кеңестер» Haber TM шабуылдарының егжей-тегжейлері мен қорғау механизмдері туралы мақалаларды оқып шығуды ұсынамыз . [2] «Ортадағы адам туралы (MitM) шабуылы» «Ортадағы адам» шабуылының теориялық және практикалық аспектілеріне, сондай-ақ олардың алдын алу әдістеріне арналған аналитикалық материал. [2] “Ортадағы адам (MITM) шабуылы дегеніміз

не? Анықтамасы және алдын алу” MITM шабуылдарының сипатын түсіндіретін және олардың алдын алу шараларын ұсынатын мақала. [1] "Орта шабуылдардағы адам (MIMA) дегеніміз не?"

MITM шабуылдарының сипатын және олармен байланысты тәуекелдерді сипаттайтын ICANN ұсынған материал. [3]

Man-in-the-Middle (MITM) шабуылдары ақпараттық қауіпсіздікке үлкен қауіп төндіреді. Төменде мұндай шабуылдардың іс жүзінде қалай жүзеге асырылғанын көрсететін кейбір нақты жағдайлар берілген:

1. Comcast Ad Embedding: 2014 жылы Comcast пайдаланушылар кірген веб-беттерге өзінің JavaScript кодтарын енгізу үшін MITM әдістерін пайдаланғаны анықталды. Бұл компанияға өзінің жарнамалары мен хабарламаларын үшінші тарап веб-беттерінің үстінде көрсетуге мүмкіндік беріп, пайдаланушының құпиялылығы мен қауіпсіздігіне қатысты алаңдаушылық туғызды. [3]

2. Lenovo ноутбуктеріндегі Superfish оқиғасы: 2014 жылы Lenovo өз ноутбуктерінде Superfish Visual Search бағдарламалық құралын алдын ала орнатқан. Бағдарламалық жасақтама шифрланған HTTPS трафигін ұстау үшін MITM шабуылын қолданды, бұл пайдаланушылардың іздеу нәтижелеріне өз жарнамаларын енгізуге мүмкіндік берді. Мұндай араласу пайдаланушылардың жеке деректерінің бұзылу қаупіне ұшырады. [4]

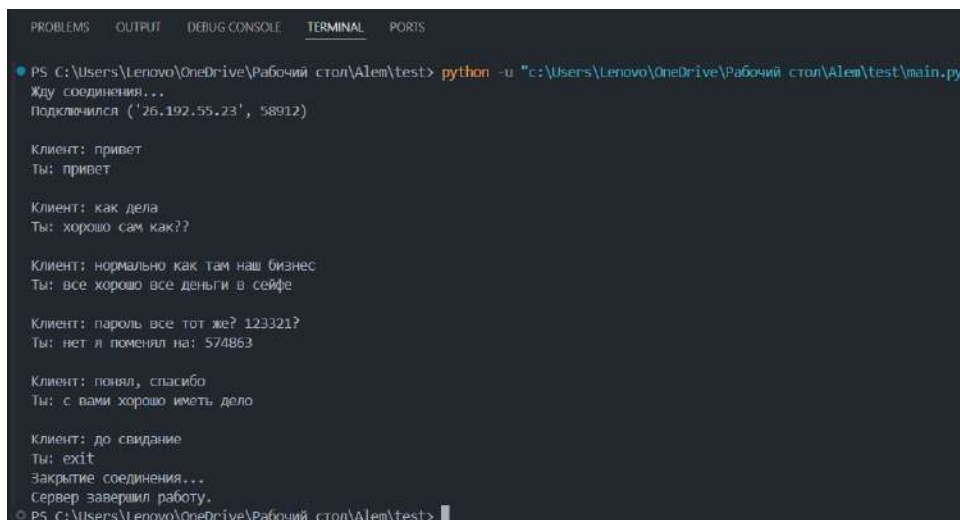
3. Ұлыбритания теміржол вокзалындағы Wi-Fi шабуылы: 2024 жылдың тамыз айында Ұлыбританияның ірі теміржол вокзалдарында жолаушылар тегін Wi-Fi желісіне қосылу кезінде террористік қауіптерге қатысты хабарларға тап болды. Тергеу нәтижесінде Wi-Fi провайдерінің қызметкері рұқсат етілмеген өзгертулер енгізіп, нәтижесінде мұндай хабарламалар пайда болғаны анықталды. [5]

4. Испаниядағы қаржылық алаяқтық: 2025 жылдың ақпанында Испанияның Алькала-де-Хенарес қаласында MITM алаяқтық жасағаны үшін ер адам қамауға алынды. Ол қызмет көрсетушінің электрондық пошта мекенжайын қолдан жасап, төлеуші компанияны басқа банк шотына шамамен 175 000 еуро аударуға көндірді, бұл айтарлықтай қаржылық шығын келтірді. [6]

Жоғарыда қарастырылған MITM шабуылын мысал ретінде қарастырдық.

Зерттеу барысында біз MITM шабуылын жасау үшін Radmin VPN қосымшасы арқылы виртуалды локальды желі құрдық.

1 - суретте сервер қосымшасының интерфейсі көрсетілген. Сервер клиенттен қосылуды күтеді. Клиент қосылғаннан кейін олардың арасында хабарламалар алмасылады. Әрбір клиент жіберген хабарлама экранға шығады және сервер оған жауап қайтарады.



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\Lenovo\OneDrive\Рабочий стол\Alem\test> python -u "c:\Users\Lenovo\OneDrive\Рабочий стол\Alem\test\main.py"
Жду соединения...
Подключился ('26.192.55.23', 58912)

Клиент: привет
Ты: привет

Клиент: как дела
Ты: хорошо сам как??

Клиент: нормально как там наш бизнес
Ты: все хорошо все деньги в сейфе

Клиент: пароль все тот же? 123321?
Ты: нет я поменял на: 574863

Клиент: попыл, спасибо
Ты: с вами хорошо иметь дело

Клиент: до свидание
Ты: exit
Закртие соединения...
Сервер завершил работу.
PS C:\Users\Lenovo\OneDrive\Рабочий стол\Alem\test>
```

1-сурет. В (сервер) көрінісі

Код құрылысы:

Сервер сокетін құру (порт 9000):

Клиенттің қосылуын күту

Клиент қосылды (IP, портты көрсету)

Әңгімелесу циклі:

Клиенттен хабарлама алу

Егер хабарлама жоқ болса, байланысты жабу

Хабарламаны экранға шығару

Сервер (сен) хабарлама жазу

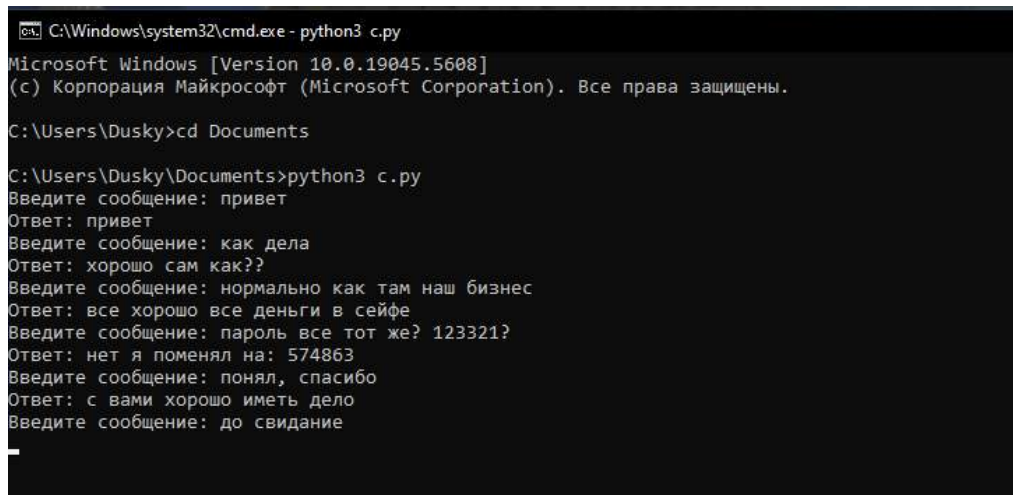
Егер хабарлама "exit" болса, байланысты жабу

Хабарламаны клиентке жіберу

Егер байланыс үзілісі болса, қатені шығарып, байланысты жабу

Сервердің жұмысын тоқтату

2 - суретте клиенттің қосымша интерфейсі көрсетілген. Клиент сервермен байланыс орнатады, содан кейін хабарламалар енгізіп серверге жіберіп отырады. Сервердің жауабын қабылдап, экранға шығарады.



```
C:\Windows\system32\cmd.exe - python3 c.py
Microsoft Windows [Version 10.0.19045.5608]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Dusky>cd Documents

C:\Users\Dusky\Documents>python3 c.py
Введите сообщение: привет
Ответ: привет
Введите сообщение: как дела
Ответ: хорошо сам как??
Введите сообщение: нормально как там наш бизнес
Ответ: все хорошо все деньги в сейфе
Введите сообщение: пароль все тот же? 123321?
Ответ: нет я поменял на: 574863
Введите сообщение: понял, спасибо
Ответ: с вами хорошо иметь дело
Введите сообщение: до свидание
```

2-сурет. А (клиент) көрінісі

Код құрылысы:

Сервермен байланыс орнату (IP: 26.49.11.123, порт: 9000):

Әңгімелесу циклі:

Хабарламаны енгізу

Хабарламаны серверге жіберу

Серверден жауап алу

Жауапты экранға шығару

3 - суретте хакердің MITM шабуылын іске асыратын интерфейсін көрсетілген. Ол ARP spoofing арқылы клиент пен сервер арасындағы хабарламаларды тыңдап, олардың арасында жүретін ақпаратты көре алады.

```
Администратор: Командная строка

C:\Users\xqtkk\Downloads>python3 "client c.py"
[+] Запускаем ARP Spoofing...
[+] Запускаем перехват трафика...
[+] Перехватываем трафик на интерфейсе Radmin VPN...
Сообщение A -> B: привет
Сообщение B -> A: привет
Сообщение A -> B: как дела
Сообщение B -> A: хорошо сам как??
Сообщение A -> B: нормально как там наш бизнес
Сообщение B -> A: все хорошо все деньги в сейфе
Сообщение A -> B: пароль все тот же? 123321?
Сообщение B -> A: нет я поменял на: 574863
Сообщение A -> B: понял, спасибо
Сообщение B -> A: с вами хорошо иметь дело
Сообщение A -> B: до свидание
[!] Остановка перехвата.
```

3-сурет. С (хакер) көрінісі

Код құрылысы:

Бастапқы параметрлер:

Клиенттің (А) және сервердің (В) IP-адрестерін көрсету  
VPN интерфейсін таңдау (Radmin VPN)

ARP Spoofing процесін іске қосу:

Әр 2 секунд сайын қайтала:

Клиентке жалған ARP жауап ("мен сервермін")

Серверге жалған ARP жауап ("мен клиентпін")

Трафикті ұстау және өңдеу:

Желіден пакетті ұстап алу

Егер пакет TCP 9000 портына бағытталған болса:

Пакеттің бағытын анықтау (A→B немесе B→A)

Пакет мазмұнын экранға шығару (хабарлама)

Пакетті қайта жинап, қарсы тарапқа жіберу (байланысты сақтау)

Процесті тоқтату (пернетақтадан сигнал берілгенде)

Қалай іске асырылды:

Жүйеде үш негізгі түйін жұмыс істейді:

- Сервер (В) клиенттің қосылуын күтіп, байланыс орнатады.
- Клиент (А) серверге қосылып, хабарлама алмасады.
- Хакер (С) ARP spoofing техникасын пайдаланып, клиент пен сервер арасында

деректерді ұстап, бақылауға алады.

Бұл арқылы хакер (С) клиент (А) мен сервер (В) арасындағы барлық сөйлесуді көре алады және қажетті ақпаратты оңай ала алады.

Төмендегі шаралар арқылы MITM (Man-in-the-Middle) шабуылдарының тәуекелін айтарлықтай төмендетуге болады:

1. Шифрлауды қолдану:

- HTTPS протоколын пайдаланыңыз, SSL/TLS сертификаттарын қолданыңыз.
- Күшті шифрлау алгоритмдерін қолданыңыз.

2. ARP spoofing-тен қорғану:

• Желілік деңгейде ARP spoofing-ке қарсы ARP inspection, DHCP snooping, IP Source Guard сияқты механизмдерді қолданыңыз.

- Статикалық ARP-кестесін қолданыңыз (тек сенімді желілерде мүмкін).
3. VPN-ды қолдану:
    - VPN арқылы барлық деректерді шифрлап, сенімді арналар арқылы жіберіңіз.
    - Сенімді VPN қызметтерін қолданыңыз.
  4. Қауіпсіз желілерді пайдалану:
    - Ашық Wi-Fi желілерін пайдаланбаңыз немесе қолданған жағдайда VPN қосылыңыз.
    - Қауіпсіздік шаралары бар және сенімді желілерді қолданыңыз.
  5. Бағдарламалық қамтамасыз етуді жаңарту:
    - Қолданылатын бағдарламалық жасақтамаларды (операциялық жүйелер, браузерлер және т.б.) үнемі жаңартып отырыңыз.
    - Жаңартуларда анықталған осалдықтар жөнделеді.
  6. Қауіпсіздік саясаттарын енгізу:
    - Желіде қауіпсіздік саясатын қолданыңыз.
    - Қызметкерлерді MITM шабуылдары туралы ескертіп, ақпараттық қауіпсіздікке үйретіңіз.

#### Қорытынды

MITM шабуылы – шабуылдаушы тараптың клиент пен сервер арасындағы деректер алмасуын ұстап алу, өзгерту немесе бағыттау арқылы жүзеге асырылатын қауіпті кибершабуылдардың бірі. Бұл зерттеуде біз MITM шабуылының негізгі түрлерін, олардың нақты өмірдегі мысалдарын және шабуылдарды іске асыру әдістерін қарастырдық.

Симуляцияда Radmin VPN көмегімен виртуалды желі құрып, ARP spoofing әдісі арқылы MITM шабуылын модельдедік. Эксперимент нәтижелері көрсеткендей, егер тиісті қорғаныс шаралары қолданылмаса, шабуылдаушы желідегі ақпаратты оқып, өзгерте алады.

MITM шабуылдарынан қорғану үшін келесі қауіпсіздік шараларын қолдану қажет: шифрлау (SSL/TLS), ARP spoofing-тен қорғану әдістері, VPN қолдану, қауіпсіз желілерге қосылу, бағдарламалық жасақтаманы үнемі жаңарту және қауіпсіздік саясаттарын енгізу.

Зерттеу нәтижелері MITM шабуылының күрделілігін және оған қарсы қорғандың маңыздылығын тағы да дәлелдейді. Ақпараттық қауіпсіздікті қамтамасыз ету үшін тиісті шараларды уақытылы қабылдау қажет.

#### Қолданылған әдебиеттер тізімі;

1. Что такое атаки типа «злоумышленник в середине» или, как их еще называют, атаки посредника (Man in the Middle Attack, MIMA)? (<https://www.icann.org/ru/blogs/details/what-is-a-man-in-the-middle-attack-2-11-2015-ru>)
2. Все об атаке “Человек по середине” (Man in the middle, MitM) [https://www.anti-malware.ru/analytics/Threats\\_Analysis/man-in-the-middle-attack](https://www.anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack)
3. Man-in-the-middle attack ([https://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](https://en.wikipedia.org/wiki/Man-in-the-middle_attack))
4. Man-in-the-Middle (MITM) Attack: Definition, Examples & More (<https://www.strongdm.com/blog/man-in-the-middle-attack>)
5. Train passengers see terror messages after station wi-fi hack (<https://www.thetimes.co.uk/article/train-passengers-islamist-terror-messages-wifi-hack-ld78vqjr0>)
6. Detenido en Alcalá de Henares por hacer el “man in the middle” (<https://cadenaser.com/cmadril/2025/02/11/detenido-en-alcala-de-henares-por-hacer-el-man-in-the-middle-ser-henares>)