

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

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

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

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

ISBN 978-601-08-5373-7

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

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

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

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

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

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

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

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

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

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

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. 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

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**

Маратов Бауыржан Жанатович

maratov011@gmail.com

7М06306 “Ақпараттық қауіпсіздік жүйелері” мамандығы бойынша магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана, Қазақстан

Ғылыми жетекшісі - техника ғылымдарының кандидаты, доцент К.М. Сагиндыков

Қазіргі уақытта шабуылдаушылар корпоративтік желілерде орнатылған қорғаныс жүйелерін айналып өту немесе жүйенің осал тұстарын анықтау үшін әлеуметтік инженерия әдістерін жиі қолдануда.

Әлеуметтік инженерия – бұл әлеуметтану мен психологияны пайдалана отырып, белгілі бір нәтижеге жетуге бағытталған кеңістік, жағдайлар мен мүмкіндіктерді жасау әдістері мен технологияларының жиынтығы.

Әлеуметтік инженерия белгілі бір формада ежелгі заманнан бері қолданылып келеді. Мысалы, Ежелгі Рим мен Ежелгі Грецияда арнайы дайындықтан өткен риторларды жоғары бағалаған, олар өз қарсыластарын «қателіктеріне» сендіре алған. Бұл адамдар дипломатиялық келіссөздерге қатысып, мемлекеттік мәселелерді шешкен. Кейінірек әлеуметтік инженерияны ҰҚК сияқты арнайы қызметтер қолдана бастады. Олардың агенттері сәтті түрде өздерін басқа біреу ретінде таныстырып, мемлекеттік құпияларды білген [1].

Әлеуметтік инженерия әдістерін қолдану үлкен қаржылық шығындарды талап етпейді және оны жүзеге асырудың көптеген нұсқалары бар. Бұл әдістер зиянкестерге үлкен әрекет алаңын ұсынады.

Киберқауіпсіздік саласында құпия деректер мен желілерді қорғау көбінесе брандмауэр, шифрлау және антивирустық бағдарламалық қамтамасыз ету сияқты техникалық қорғанысқа бағытталған. Дегенмен, ұйымдық қауіпсіздікке төнетін ең кең таралған және қауіпті қатерлердің бірі бағдарламалық жасақтаманың осал тұстарын пайдаланатын хакерлерден емес, қызметкерлерді әлеуметтік инженерия арқылы манипуляциялайтын жеке тұлғалардан туындайды. Бұл психологиялық манипуляция адамдарды құпия ақпаратты ашуға, рұқсат етілмеген қол жеткізуге немесе қауіпсіздікке нұқсан келтіретін әрекеттерді орындауға алдауға бағытталған. Әлеуметтік инженерия тәуекелін тиімді азайту үшін қызметкерлерді қорғау және оқыту әдістері маңызды болып табылады.

Қызметкерлер әлеуметтік инженериядан қорғаныстың бірінші желісі ретінде осы шабуылдарды тану және оларға қарсы тұру үшін білім мен құралдармен қамтамасыз етілуі керек. Тиісті қорғаныс болмаса, ұйымдағы адамдар абайсызда шабуылдаушыларға құпия деректерге, жүйелерге немесе физикалық орындарға кіру мүмкіндігін бере алады. Әсері жойқын болуы мүмкін, соның ішінде қаржылық жоғалту, беделге нұқсан келтіру, заңды жауапкершіліктер және тұтынушы сенімінің жоғалуы.

Ұйымдар технологиялық қауіпсіздік шаралары маңызды болғанымен, компания активтерін қамтамасыз етуде адам элементі маңызды рөл атқаратынын мойындауы керек. Қызметкерлерді хабардар ету және қорғау стратегияларына инвестициялау арқылы бизнес әлеуметтік инженерлік шабуылдарға осалдығын айтарлықтай төмендете алады [2].

Әлеуметтік инженериямен күресудің негізгі оқыту әдістері:

1. Фишинг модельдеулері және хабардар ету науқандары

Қызметкерлерді фишингтік шабуылдар арқылы жүйелі түрде тестілеу оларға әдеттен тыс жіберушінің мекенжайлары, күдікті сілтемелер немесе жеке ақпаратқа арналған шұғыл сұраулар сияқты фишингтік электрондық хабарлардың жасырын белгілерін тануға көмектеседі. Бұл жаттығулар қызметкерлерге қырағылық танытуға және киберқылмыскерлердің мінез-құлқын манипуляциялау үшін қолданатын әдістерді түсінуге көмектеседі. Ақпараттық науқандар қажетсіз электрондық пошталарға, телефон

қоңырауларына немесе хабарламаларға деген дұрыс күмәнділікке ықпал етуі керек.

2. Қауіпсіздік саласындағы үздік тәжірибелер бойынша тренинг

Қызметкерлер құпия ақпаратты өңдеу кезінде ең жақсы тәжірибелерді қалай қолдану керектігін үйретуі керек. Бұған күшті құпия сөздерді орнату, ақпаратқа күдікті сұрауларды тану және құпия құжаттарды қауіпсіз жою бойынша нұсқаулар кіреді. Оқыту сонымен қатар құпия деректер мен жүйелерге қол жеткізуге арналған сұрауларды қалай өңдеу керектігін және сұраушының заңдылығын әрқашан тексеруді қамтуы керек, әсіресе олар сыртқы немесе бейтаныс болса.

3. Рөлдік оқыту

Ұйымдағы әртүрлі рөлдер әртүрлі әлеуметтік инженерлік шабуылдарға тап болуы мүмкін. Мысалы, басшылар мен жоғары деңгейлі қызметкерлер жиі фишингтік шабуылдарға ұшырайды, ал тұтынушыларға қызмет көрсететін қызметкерлер сылтауларға көбірек бейім болуы мүмкін. Оқытуды нақты жұмыс функцияларына бейімдеу қызметкерлердің ең ықтимал әлеуметтік инженерлік шабуыл түрлеріне дайын болуын қамтамасыз етеді.

4. Қауіпсіздік – бірінші мәдениетті құру

Проактивті қауіпсіздік мәдениеті әлеуметтік инженерлік шабуылдардың сәттілігін айтарлықтай төмендетуі мүмкін. Қызметкерлерді күдікті әрекеттер туралы дереу және кек алудан қорықпай хабарлауға шақырыңыз. Қызметкерлерге ықтимал қауіпсіздік тәуекелдері туралы алаңдаушылық білдіру үшін қауіпсіз орта жасау пайда болатын қауіптерге тезірек жауап беруді қамтамасыз етеді.

5. Үнемі біліктілікті арттыру курстары

Әлеуметтік инженерия тактикасының ландшафты үнемі дамып отырады. Шабуылшылар өз техникаларын үнемі жетілдіріп отырады, сондықтан қызметкерлерді оқыту бір реттік оқиға болмауы керек. Қызметкерлердің соңғы қауіптермен және олармен күресу жолымен жаңартылғанын қамтамасыз ету үшін біліктілікті арттыру курстары мерзімді түрде өткізілуі керек.

6. Симуляцияланған әлеуметтік инженерия сценарийлері

Қызметкерлер имитацияланған әлеуметтік инженерлік шабуылдарға жауап беруі керек болатын тікелей сценарийлерді іске қосу (жеке немесе онлайн болсын) қызметкерлерге жылдам шешім қабылдауға және үйренгендерін бекітуге көмектеседі. Бұл қызметкерлерге басқарылатын ортада нақты жағдайдың қысымын сезінуге мүмкіндік береді, бұл оларға нақты қауіпке тап болған кезде тиімді әрекет ету жолын жақсырақ түсінуге мүмкіндік береді.

7. Көп факторлы аутентификацияны (КФА) пайдалануды ынталандыру

Оқытумен тікелей байланысты болмаса да, көп факторлы аутентификацияны (КФА) енгізу әлеуметтік инженерлік шабуылдарының әсерін айтарлықтай төмендетеді. Тіпті шабуылдаушылар қызметкердің желіге кіру, тіркеу деректерін сәтті алса да, СІМ қамтамасыз ететін қауіпсіздіктің қосымша деңгейі, рұқсатсыз кіруді қиындатады.

Оқытудың тиімділігін өлшеу

Оқыту үрдісін қамтамасыз ету жақсы нәтижеге жеткізуге жеткіліксіз - ұйымдар қауіпсіздік туралы хабардар ету бағдарламаларының тиімділігін үнемі бақылап отыруы қажет. Сәтті фишингтік модельдеу жылдамдығы, хабарланған қауіпсіздік оқиғаларының саны және қызметкерлердің кері байланысы сияқты көрсеткіштер оқу әрекеттерінің сәттілігі туралы құнды түсініктерді бере алады. Оған қоса, қауіпсіздіктің нақты бұзылуының немесе әлеуметтік инженерлік шабуылдардың әрекет ету үрдістерін қадағалау оқу процесінде жақсарту аймақтарын анықтауға көмектеседі [3].

Сондай-ақ, әлеуметтік инженерия әдістері классикалық бұзу әдістерінен айырмашылығы ескірмейді. Қорғаныс саласында да, шабуылда да жаңа трендтер мен жаңалықтарды үнемі бақылап отыру қажет, өйткені олар арқылы қажетті әрекеттерді жүзеге асыруға болады.

Дегенмен, барлық әлеуметтік инженерлер алаяқтар емес. Олар бәсекелестердің шабуылы немесе қара пиардан кейін компанияның беделін қалпына келтіруге көмектесуі мүмкін. Мысалы, психологиялық әдістер, анонимді пікір қалдырушының деректерін алып, оны қажетсіз пікірлер мен жалған ақпаратты жоюға итермелеу үшін қолданылады.

Әлеуметтік инженерлер форумдарға тіркеліп, теріс пікірдегі аудиториямен диалог жүргізеді және нейролингвистикалық программалау техникаларын қолданып, олардың пікіріне әсер етеді.

Қауіптің алдын алу тәсілдерін анықтау үшін, киберқылмыскерлер не істей алатынын және оны қалай жүзеге асыратынын түсіну қажет [4].

Біріншіден, адаммен хат алмасу арқылы сенімге кіріп, болашақ шабуылдарға қажет болатын ақпаратты білуге болады. Мысалы, басқа қызметкерлердің телефон нөмірлері мен электрондық пошталары, желінің конфигурациясы, қорғаныс құралдарының нұсқалары сияқты мәліметтер.

Екіншіден, күдік тудырмайтын «жұмыс кестесі», «шот бойынша қарыз», «жұмыстан босату» сияқты зиянды файлды ашқан кезде, компьютерге жұқпалы файл орнатылады. Нәтижесінде қылмыскер жүйеге қол жеткізе алады.

Тағы бір шабуыл әдісі – «кері әлеуметтік инженерия». Мұндай шабуылдың мысалы ретінде қорғалатын аймаққа тазалаушы ретінде кіруді айтуға болады. Сіз қабырғадағы техникалық қолдау нөмірін өзіңіздің нөміріңізге ауыстырасыз, содан кейін кішігірім ақау жасайсыз. Бір күннен кейін, көңілсіз пайдаланушы сізге қоңырау шалып, өз білімін «білікті маманмен» бөлісуге дайын болады. Авторизацияңыз күдік тудырмайды, өйткені адам кімге және не үшін хабарласқанын біледі.

Әлеуметтік инженерия салдарынан құпия ақпараттың таралу ықтималдығын азайту үшін келесі ережелерді сақтау қажет:

- Ақпараттық қауіпсіздік мамандары орындалатын, жүйелік және басқа да файлдарға арналған кеңейтімдері бар файлдарды жіберуге тыйым салуы қажет. Сондай-ақ, компьютерлік сауаттылықты арттыру мақсатында персоналмен нұсқаулықтар өткізілуі керек.

- Хатқа қосымша немесе сілтеме келген жағдайда, жіберушінің мекенжайын, хаттың кеңейтімін мұқият тексеріп, файлды антивирустық бағдарламалық қамтамасыз ету арқылы сканерлеу қажет.

- Қылмыскермен байланысқа түспеу маңызды, себебі ол әңгіме барысында келесі құрбанына шабуыл жасау үшін қажетті ақпаратты алуы мүмкін.

Әлеуметтік инженерия бүгінгі күні ұйымдардың алдында тұрған ең жасырын қауіпсіздік қатерлерінің бірі болып қала береді. Ол адам психологиясын пайдалана отырып, оны тіпті ең озық техникалық қорғаныс құралдарының алдын алуға тырысатын шабуыл векторына айналдырады. Күшті, қызметкерлерді қорғау және оқыту бағдарламаларына инвестициялау арқылы, ұйымдар әлеуметтік инженерлік шабуылдарды танитын және оларға қарсы тұруға жақсырақ дайындалған, қауіпсіздікті білетін, жұмыс күшін құра алады. Қызметкерлер киберқылмыскерлер қолданатын тактиканы түсінгенде және оларға тиімді әрекет ету құралдары берілгенде, олар осы дамып келе жатқан қауіптерден ұйымның бірінші және ең тиімді қорғаныс желісі болады [5].

Жұмыс қорытындысы бойынша, әлеуметтік инженерия көмегімен жасалатын шабуылдардың негізгі әдістері ұсынылды. Сонымен қатар, осы типтегі шабуылдардың алдын алу үшін негізгі принциптер тұжырымдалды, және сол принциптер негізінде персоналды дайындау қажет.

Қолданылған әдебиеттер тізімі

1. Әлеуметтік инженерия және әлеуметтік хакерлер / М.В. Кузнецов, И.В. Симдянов. СПб.: БХВ-Петербург, 2007.

2. Positive research. Практикалық қауіпсіздік бойынша зерттеулер жинағы. [Электрондық ресурс]. Қол жеткізу режимі: <https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2017-rus.pdf/>
3. Алдау өнері / Кевин Митник, Уильям Саймон. М.: ВМиК МГУ баспа бөлімі. МАКС Пресс баспасы, 2018.
4. Whitman, M. E., & Mattord, H. J. (2020). *Principles of Information Security* (6th ed.). Cengage Learning.
5. Symantec Corporation**. (2020). *2019 Internet Security Threat Report*. Symantec.
- A detailed annual report that highlights trends in cybersecurity threats, including social engineering. It provides real-world case studies and advice on securing employees from these types of attacks. [Link: <https://www.broadcom.com/company/newsroom/press-releases?filtr=internet-security-threat-report>]

УДК: 004.056.5

WEBSOCKET ПРОТОКОЛЫНДАҒЫ ОСАЛДЫҚТАРДЫ ТАЛДАУ

Мағзумов Алихан Маратұлы

alihan.magzumov@mail.ru

Л.Н.Гумилев атындағы ақпараттық қауіпсіздік факультетінің магистрантты
Ғылыми жетекші – Ж.Сауханова

Аннотация: Бұл мақалада WebSocket протоколының осалдықтарын зерттеу және талдау әдістері қарастырылады. Нақты шабуыл мысалдары негізінде WebSocket байланыстарының қауіпсіздік мәселелері талданып, олардың ақпараттық жүйелерге ықтимал әсері бағаланады. Сондай-ақ осалдықтарды пайдаланудың негізгі әдістері мен оларды анықтау жолдары көрсетіледі. WebSocket байланыстарын қорғау және шабуылдардың алдын алу бойынша ұсыныстар беріледі. Мақала ақпараттық қауіпсіздік саласындағы мамандарға, зерттеушілерге және веб-қосымшалар әзірлеушілеріне арналған.

Кілт сөздер: Веб-қосымша, Интернет-ресурс, Websocket, қауіпсіздік, осалдық, ақпарат жинау.

Ақпараттық қауіпсіздіктегі осалдық - шабуылдаушылар қолдана алатын ақпараттық активтің немесе бақылау мен басқарудың әлсіз жақтары. Ақпараттық қауіпсіздіктің осалдықтарының жіктелуі өте көп. Соның ішінде веб-қосымшалардағы Websocket осалдықты ескерген жөн. Өйткені бұл қосымшаның және онымен байланысты деректердің құпиялылығына, тұтастығына және қол жетімділігіне нұқсан келтіруі мүмкін қауіпсіздік қатерлері мен шабуылдарына жол береді.

WebSocket осалдықтарын және олардың веб-қосымшалар үшін салдарын зерттеу әдістемесі теориялық талдауды және қауіпсіздік әдістерін әзірлеуді біріктіретін кешенді тәсілді қамтиды.

WebSocket – бұл екі жақты нақты уақыттағы деректер алмасуды қамтамасыз ететін хаттама. Ол веб-қосымшалардағы жылдамдық пен тиімділікті арттырады, бірақ сонымен бірге жаңа қауіпсіздік қатерлерін де тудырады. WebSocket хаттамасының ерекшелігі – тұрақты қосылым орнату арқылы сервер мен клиент арасында үздіксіз байланыс жасауында. Бұл механизм дәстүрлі HTTP сұраныс-жауап үлгісінен ерекшеленеді және дұрыс қорғалмаған жағдайда осалдықтарға жол ашады.