

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 «IoT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

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

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «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. Раматуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

6. М. С. Абдуллаев, Linux жүйелеріндегі ақпараттық қауіпсіздікті қамтамасыз ету негіздері, Алматы, 2017.

7. Е. А. Нұрғалиев, Операциялық жүйелер қауіпсіздігі: тәсілдер мен құралдар, ISBN 978-5-4468-9708-7, 2019.

8. Қ. С. Иманбаев, Linux жүйелерін шабуылдардан қорғау әдістері, Алматы техникалық университеті, 2020.

УДК 004.056.5

ЗАМАНАУИ ФИШИНГ ТҮРЛЕРІ МЕН ОЛАРДЫҢ ҰЙЫМДЫҚ АҚПАРАТТЫҚ ЖҮЙЕЛЕРГЕ ЫҚПАЛЫ

Қадыр Нұртілеу Ермекұлы

dnurtu@mail.ru

Л.Н.Гумилев атындағы Еуразия ұлттық университетінің «Ақпараттық технологиялар» факультетінің магистранты, Астана қ., Қазақстан
Ғылыми жетекші: ф-м. ғ.к., доцент Сауханова Ж. С.

Аңдатпа. Бұл мақалада заманауи фишинг шабуылдарының жаһандық және Қазақстандағы динамикасы, жаңа әдістері мен ұйымдық ақпараттық жүйелерге әсері қарастырылады. Фишингтің эволюциясы, әлеуметтік инженерия әдістерімен байланысы және жасанды интеллект пен deepfake технологияларын қолдану арқылы күрделенуі жан-жақты талданады. Сонымен қатар, фишингтен қорғаудың кешенді техникалық, ұйымдастырушылық және заңнамалық шаралары ұсынылады.

Түйін сөздер: фишинг, әлеуметтік инженерия, smishing, vishing, deepfake, ақпараттық қауіпсіздік, жасанды интеллект.

Кіріспе

Фишинг – интернеттегі алаяқтықтың ең кең тараған түрлерінің бірі. Онда қаскүнемдер өзін сенімді ұйымның немесе адамның атынан таныстырып, пайдаланушыны алдап құпия деректерін (логин, құпиясөз, банк картасы мәліметтері, т.б.) өз қолымен беруіне мәжбүрлейді. 2024–2025 жылдары қашықтан жұмыс істеу мен бұлттық сервистердің кең таралуы фишинг шабуылдарының ауқымын бұрынғыдан бетер ұлғайтты, шабуылдар саны мен күрделілігі үздіксіз өсуде. Бұл мақалада заманауи фишинг шабуылдарының статистикасы, жаңа түрлері, маңызды оқиғалары мен олардан қорғану стратегиялары талданады.

Талдау және зерттеу нәтижелері

1. Әлемдік және Қазақстандағы фишинг шабуылдары динамикасы (2024–2025)

1.1 Әлемдік үрдістер

Фишинг шабуылдары ең көп бағытталған секторлар – әлеуметтік желілер мен онлайн қызметтер. 2024 жылы фишингтің 30.5%-ы әлеуметтік медиа платформаларына бағытталды[1]. Әлеуметтік желі аккаунттарын бұзу фишерлердің басты мақсаты болып қала берді. Одан кейінгі нысана – **онлайн қызметтер мен пошталар (SAAS/Webmail, ~21%)**[1][3], ал **қаржы секторына** жасалған шабуылдар жалпы фишинг оқиғаларының 13%-ын құрады[3]. 2024 жылы қаржы және сақтандыру саласына бағытталған фишинг 27.8%-ға жетіп, жылдық өсім 393%-ды көрсетті[2]. Сонымен қатар, электронды коммерция (8%), телекоммуникация (5%), логистика және жол жүру салалары да фишерлер назарында[3].

Фишингтің жалпы өсім қарқыны алаңдатарлық: Verizon DBIR 2023 дерегінше, әлеуметтік инженерия шабуылдарының 83%-ы фишингпен байланысты[4]. 2024 жылы SMS-фишинг (smishing) саны тоқсандық есепте 22%-ға артты[1], ал телефон арқылы алдау (vishing) оқиғалары 28%-ға көбейді[9]. 2023 жылы фишинг жылдық есеппен 60%-ға өсті[2], ал зиянды хаттар жаһандық пошта трафигінің 1.2%-ын құрады, бұл күніне 3.4 миллиард фишинг хат деген сөз[4]. Жалпы алғанда, соңғы мәліметтер фишингтің жыл сайын екі таңбалы пайыздарға өсіп отырғанын және жаңа тактикалардың пайда болуымен оның тиімділігі де артып келе жатқанын айғақтайды (Кесте 1).

Көрсеткіш (Global)	Маңыздылығы / Мәліметтер
Фишингтік шабуылдар саны (Q3 2024)	932 923 (жүзеге асқан оқиға)[9]
2023–2024 өсім қарқыны	≈ +60% (жылдық жаһандық өсім)[2]
Блокталған фишинг хаттары және сілтемелері (2024)	893 млн әрекет (Kaspersky дерегі)[3]
Ең көп нысанаға алынған сала	Әлеуметтік желілер (30.5%)[11]
Ең көп имитацияланған бренд	Microsoft (43.1% шабуылда)[2]

Кесте 1. Әлемдегі фишинг шабуылдарының негізгі көрсеткіштері, 2024 жыл

1.2 Қазақстандағы жағдай

Қазақстанда фишингтен зардап шегуші секторлар қатарында қаржы ұйымдары мен мемлекеттік мекемелер бар. Мысалы, 2024 жылдың бірінші жартысында еліміз қаржы секторына бағытталған кибершабуылдар үлесі бойынша әлемде 10-орында болды[5]. Банктерге қарсы шабуылдардың 85%-ында трояндық бағдарламалар қолданылса, сонымен бірге көптеген жағдайда пайдаланушыларға жалған хаттар мен сілтемелер жіберілген[5]. Жалпы алғанда, Қазақстандағы киберинциденттердің **53%-ында әлеуметтік инженерия әдістері** (соның ішінде фишинг) пайдаланылғаны тіркелді[10]. KZ-CERT сарапшылары мемлекеттік және квазимемлекеттік секторға жасалған шабуылдардың да көбейгенін байқаған – әсіресе жалған мемлекеттік сайттар немесе қызметтер атын жамылып жасалатын фишинг оқиғалары[6]. Қазақстан ұйымдары арасында жүргізілген сауалнама нәтижесінде әр үш компанияның біреуі кибершабуылға ұшырағанын, ал деректердің сыртқа шығу оқиғаларының **25%-ы қызметкерлердің фишингтік алдауға түсуінен** болғанын көрсетті[5]. Бұл статистика елімізде кадрлардың кибергигиена деңгейін көтеру қажеттігін және ұйымдардың фишингтен қорғану шараларын күшейту керектігін аңғартады (Кесте 2).

Көрсеткіш (Қазақстан)	Маңыздылығы / Мәліметтер
Тіркелген фишинг оқиғалары (2023)	~ 2 200 оқиға[5]
2024 ж. өсім (қаңтар-сәуір 2023-пен салыстырмалы)	+650% (7.5 есеге көбейген)[5]
Интернет-алаяқтықтан келген шығын (2023)	17.5 млрд ₸ [7]
Деректер бұзылуына фишингтің үлесі (2024)	25% [5]
Әлеуметтік инжиниринг қолданылған шабуылдар үлесі	53% [10]

Кесте 2. Қазақстандағы фишингке қатысты деректер

2. Фишинг шабуылдарының жаңа түрлері және әдістері

2.1 Жасанды интеллект қолданылатын фишинг

Жасанды интеллект (AI) технологиялары фишингті жаңа деңгейге көтерді. **Генеративті нейрожелілер** алаяқтарға өте нанымды алдау мәтіндерін жаппай жасауға мүмкіндік беріп отыр. Сарапшылар **2023–2024** жылдары **AI** арқылы жасалған фишинг компанияларының күрт артқанын атап өтеді[2]. Фишинг хаттарының тілі мен мазмұны құрбан профиліне бейімделіп, **ChatGPT** сияқты құралдар арқылы дайындалады. Нәтижесінде **грамматикалық және стилистикалық мінсіз**, сенім тудыратын алдау хаттары пайда болып, тіпті тәжірибелі қолданушыларды да жаңылыстырады. **AI** сонымен бірге әлеуетті

құрбандардың әлеуметтік желідегі белсенділігін, қызығушылықтарын талдап, нысаналы **spear-phishing** хаттарын автоматты түрде жасайды.

Дауыстық және мәтіндік фишинг те **AI** көмегімен өршіп отыр. **2024 жылы** телефон арқылы алдау (**vishing**) және SMS арқылы алдау (**smishing**) оқиғалары рекордтық деңгейге жетті[9]. **AI-модельдер** қоңырау кезінде адамның дауысын, сөйлеу мәнерін айнытпай салады. Мысалы, **Hiya** дерегі бойынша, АҚШ, Канада және Еуропа тұрғындарының үштен бірі **AI** арқылы жасалған жалған қоңырауға тап болып, олардың ~30%-ы алданған[12]. Осындай «ақылды» қоңыраулардың салдары ауыр – қарапайым телефон алаяқтығында орташа **\$539** жоғалса, **AI-генерацияланған** алаяқтықта бұл сома **\$6000**-нан асады[12]. Бұл **AI**-дың дәстүрлі әдістерге қарағанда әлдеқайда қауіпті екенін дәлелдейді.

Фишингті «қызмет ретінде» ұсыну да кең етек жайды. Даркнетте фишингті жеңілдететін **Phishing-as-a-Service** платформалары пайда болды. **AI**-дың қолжетімділігі оны тіпті **техникалық білімі төмен** алаяқтарға да қолайлы етті. Дайын **фишинг-комплекттер, боттар мен скрипттер** ашық сатылып, тіпті **әлеуметтік инженерия сценарийін** де **AI** автоматты түрде дайындайды. Нәтижесінде фишинг шабуылдары **сандық және географиялық** тұрғыда бұрынғыдан да кең таралды, енді бұл тек дамыған елдердің мәселесі емес, **киберқауіпсіздік деңгейі төмен** елдерге де қауіп төндіруде.

2.2 Deepfake технологиялары арқылы алдау

Deepfake-видео және аудио – әлеуметтік инженерияның жаңа қаруы. **Deepfake** – нейрожелі арқылы жасалған **жалған бейне немесе дауыс**, алаяқтық пен манипуляция үшін қолданылады. **2024 жылы** deepfake технологияларымен жасалған алаяқтықтар ерекше резонанс тудырды.

Ұлыбританиядағы **Agur** компаниясында **қаскүнемдер** қаржы директоры мен қызметкерлердің бейнесін deepfake-видео арқылы қайталап, **\$25 млн** (HK\$200 млн) заңсыз аудартқан[8]. Бұл **корпоративтік ортадағы** deepfake-алаяқтықтың қаншалықты қауіпті екенін көрсетті. **Киберқауіпсіздік басшысы** Роб Грейг ұйымдарда фишинг, **жалған шот-фактуралар** мен **WhatsApp дауыстық бұрмалау** шабуылдарының қарқынды өсіп жатқанын айтты[8].

Deepfake технологиялары **қаржылық алаяқтықтан бөлек, саяси және әлеуметтік тұрақтылыққа** да қауіп төндіруде. **2024 жылы** deepfake құралдары **сайлау науқандарына** қолданылды. АҚШ-та белгісіз біреулер **президент Джо Байденнің** дауысын бұрмалап, Нью-Гэмпшир сайлаушыларына «**праймеризде дауыс бермеуге**» шақырған **жалған робот-қоңыраулар** таратты[8]. Бұл оқиға **deepfake-тің саяси манипуляция құралына** айналғанын көрсетті.

Сондай-ақ, **АҚШ-тың Мэриленд штатында** мектеп директорының дауысы қолданылып, балағат сөздер айтылған **deepfake-аудио** тарады. Нәтижесінде, мектеп басшысы мен оның отбасы **өлім қаупі бар қоқан-лоққыларға** тап болды[8]. Бұл оқиғалар deepfake тек **қаржылық шығын** ғана емес, **қоғамдық тұрақтылыққа** да елеулі зиян келтіретінін көрсетеді.

Қорыта айтқанда, **AI және deepfake** технологиялары **фишинг шабуылдарын** жаңа деңгейге көтерді. **2024 жылы** жасанды интеллектінің көмегімен **фишинг саны мен сапасы** айтарлықтай артты – оларды анықтау қиындап, алдын алу күрделі мәселеге айналды[2]. **Киберқылмыскерлер** үздіксіз жетілдірілген құралдарды өз пайдасына асырып жатқанда, **қорғаныс шаралары** да соған сай дамуы қажет.

3. Фишингке қарсы қорғаныс стратегиялары және киберқауіпсіздікті нығайту

Фишинг шабуылдарының эволюциясы қорғаныс тәсілдерін үнемі жетілдіруді талап етеді. Ұйымдар мен мемлекеттер **техникалық, ұйымдастырушылық және заңнамалық** деңгейде кешенді шаралар қабылдауда (Сурет 1). Көптеген ұйымдар фишингтен қорғану үшін **SPF, DKIM, DMARC** секілді хат түпнұсқалығын тексеретін протоколдарды енгізіп, күмәнді

хаттарды автоматты түрде оқшаулайды. Сонымен қатар, **жасанды интеллект негізіндегі** антифишинг жүйелері желі трафигі мен хаттарды талдап, күдікті мазмұнды автоматты түрде анықтайды. Қызметкерлердің аккаунттарын қорғау үшін **қос факторлы аутентификация (2FA/MFA)** және **аппараттық қауіпсіздік токендері** (мысалы, **YubiKey**) кеңінен қолданыла бастады. Ірі IT-компаниялар мүлде **парольсіз аутентификацияға** көшуді көздеп отыр, бұл фишингті мүлдем тиімсіз етуі мүмкін.

Желілік қауіпсіздік архитектуралары да өзгеріп келеді. Соңғы жылдары кең тараған **Zero Trust** қағидасы бойынша, желіге немесе аккаунтқа әуелден ешқандай сенім артылмайды, әр әрекет қайта тексеріледі. Бұл тәсіл фишинг арқылы ішкі желіге енген зиянкестердің қозғалысын шектейді. Сонымен қатар, бұлттық **CASB** және **Secure Web Gateway** шешімдері сыртқы фишингтік сілтемелерге өту әрекеттерін автоматты түрде бақылап, қауіпті ресурстарды ашуға жол бермейді. Осы бағытта **Zscaler** секілді компаниялар ұйымдарға кешенді қауіпсіздік платформаларын ұсынып отыр[2].

Фишингке қарсы ең әлсіз буын — **адам факторы**, сондықтан қолданушыларды үнемі оқыту өте маңызды. Компаниялар тұрақты **тренингтер мен симуляциялар** өткізіп, қызметкерлерге фишинг белгілерін тануды үйретуде. Әр тоқсан сайын жалған фишинг хаттары жіберіліп, қызметкерлердің реакциясы тексеріледі: хатты дер кезінде танығандар мадақталады, ал алданып қалғандар қосымша оқытылады. Бірақ тіпті оқытылған мамандар да алдануы мүмкін, әсіресе **deepfake** қолданылған күрделі шабуылдарға қарсы тұру қиын[7]. Сондықтан көптеген ұйымдар **ірі қаржылық операцияларды** орындамас бұрын, басшының тікелей растауын (телефон немесе бейнебайланыс арқылы) талап ететін ішкі процедураларды енгізуде. Бұл көпсатылы тексеру фишинг арқылы ірі алаяқтықтардың алдын алуға көмектеседі.

Ұйымдық процестерді де жетілдіру маңызды. Ақпараттық қауіпсіздік бөлімдерінде арнайы **CSIRT/CERT** топтары құрылып, фишинг оқиғаларына жедел әрекет ету, жүйені оқшаулау, зиянды азайту және қызметкерлерге хабарлау тәрізді механизмдер автоматтандырылуда. Қазақстанда бұл бағытта **Ұлттық Банк** жанынан **Антифрод орталығы** құрылып, ол **банк транзакцияларын** бақылап, күмәнді ақша аударымдарын анықтайды. Сонымен қатар, барлық банктерге ортақ **қара тізімдер** алмасу арқылы фишингтік есепшоттарды бірлесіп бұғаттау жүйесі іске қосылды[11]. Мұндай үйлестірілген шаралар фишингтен туындайтын қаржылық шығындарды азайтуға бағытталған.

Заңнамалық деңгейде де өзгерістер бар. Қазақстанда «**Цифрлық трансформация, АКТ және киберқауіпсіздік индустриясын дамыту концепциясы (2023–2029)**» бекітіліп, оның аясында **ұлттық киберқауіпсіздік координациялық орталығын күшейту және киберполигон құру** көзделген[7]. Сондай-ақ, 2022 жылы енгізілген заңнамалық түзетулер арқылы дербес деректерді қорғау талаптары күшейтілді. Халықаралық деңгейде **AI Act** сияқты заң жобалары **deepfake** және жасанды интеллектіні жауапкершілікпен пайдалану нормаларын бекітуді көздейді[8]. Сонымен қатар, **Interpol** мен **Europol** фишингтік топтарға қарсы бірлескен операциялар ұйымдастырып, **трансшекаралық киберқылмыстарға қарсы күресті күшейтіп** келеді.

Осылайша, фишингке қарсы тиімді қорғаныс тек технологиялық шешімдермен

1-қабат: Техникалық деңгей

- Спам-фильтрлер мен анти-фишинг шешімдер
- Secure Email Gateway
- Веб-фильтрлер мен DNS қорғанысы
- Антивирус және EDR жүйелері
- Сілтемелер мен файлдарды талдау

2-қабат: Кадрлық (адамдық) деңгей

- Қызметкерлерге тұрақты оқыту
- Симуляциялық фишинг шабуылдары
- Басшылық пен IT-ді дайындау
- Күдікті хабарламаларды хабарлау жүйесі

3-қабат: Процесстік деңгей

- E-mail тексеру және бекіту процедуралары
- Ішкі саясаттар мен нұсқаулықтар
- Инциденттерге жауап беру алгоритмдері
- Үздіксіз бақылау мен аудит

ғана емес, адам капиталы, ұйымдық процестер және заңнамалық шаралар арқылы да қамтамасыз етілуі тиіс.

1-сурет. Ақпараттық жүйелерді фишингтен қорғаудың 3-қабатты қауіпсіздік деңгейі

Қорытынды

Қазіргі фишинг шабуылдары жылдам өзгеріп, жаңа әдістермен толықтырылуда. 2024–2025 жылдары әлем бойынша фишинг белсенділігінің әрі қарай өсуі болжануда, әсіресе AI және deepfake-ты қолданатын күрделі шабуылдар көбеймек[2]. Бұл тренд Қазақстанды да айналып өтпейді – елімізде интернет алаяқтық саны ұлғайып, олардың ішінде фишинг ерекше орын алуда[5]. Фишингтің эволюциясы оған қарсы кешенді жауапты талап етеді: техникалық қорғанысты күшейту, қызметкерлерді оқыту, бизнес-процестерді жетілдіру және мемлекеттік деңгейде саясат қалыптастыру – барлығы бірдей маңызды. Ғылыми зерттеулер мен сараптамалық талдаулар фишингтен қорғану құралдарының тиімділігін үнемі бағалап, жақсарту керектігін көрсетеді. Киберқауіпсіздікті нығайту – үздіксіз процесс: жаңа шабуыл түрлері пайда болған сайын, оларға төтеп беретін инновациялық шешімдер де дамып отыруы тиіс. Тек осындай жан-жақты дайындық арқылы ұйымдар өз ақпараттық жүйелерін және пайдаланушыларды фишинг қатерінен сенімді қорғай алады.

Қолданылған әдебиеттер тізімі

1. Phishing Activity Trends Report – 3rd Quarter 2024 / Anti-Phishing Working Group (APWG). – 2024. – Желтоқсан. – Қолжетімді: https://docs.awpg.com/reports/apwg_trends_report_q3_2024.pdf
2. 2024 Phishing Report – Press Release / Zscaler ThreatLabz. – 2024. – 23 сәуір. – Қолжетімді: <https://www.zscaler.com/resources/security-research/2024-phishing-report.pdf>
3. Spam and Phishing Report 2024 / Kaspersky Lab. – 2025. – Қаңтар. – Қолжетімді: <https://securelist.com/spam-and-phishing-report-2024/>
4. Top Phishing Statistics and Trends You Must Know / Keepnet Labs. – 2024. – Қолжетімді: <https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know>
5. Қазақстан қаржы секторына кибершабуылдар бойынша 10-орында // Kursiv Media. – 2024. – 14 тамыз. – Қолжетімді: <https://kursiv.kz/news/finansy/2024-08/kz-cyberattack-ranking>
6. Обзор инцидентов ИБ за I квартал 2024 года // incode.com. – 2024. – 22 сәуір. – Қолжетімді: <https://profit.kz/articles/2024-q1-cyberincidents/>
7. Digital Security and Threats in Kazakhstan // Eurasian Research Institute E-Bulletin. – 2025. – №376. – Қолжетімді: <https://www.eurasian-research.org/wp-content/uploads/2025/02/E-bulletin-04.02.2025-No-376.pdf>
8. Top 5 Cases of AI Deepfake Fraud from 2024 / Incode. – 2024. – 20 желтоқсан. – Қолжетімді: <https://www.globalsecuritymag.com/blog/top-5-ai-deepfake-frauds-2024/>
9. Phishers Target Victims in New, Intrusive Ways – Q3 2024 / APWG, Global Security Magazine. – 2024. – Желтоқсан. – Қолжетімді: <https://www.globalsecuritymag.com/phishing-trends-2024-q3.html>
10. Актуальные киберугрозы в странах СНГ 2023-2024 / Positive Technologies. – 2024. – Қолжетімді: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/>
11. Building Digital Public Infrastructure: Lessons Learned from Kazakhstan / CSIS Analysis. – 2024. – Қолжетімді: <https://www.csis.org/analysis/building-digital-public-infrastructure-lessons-learned-kazakhstan>
12. AI Deepfake Fraud Calls Dominate Q4 Scams, Costing Consumers Millions / BusinessWire. – 2025. – 25 ақпан. – Қолжетімді: <https://www.businesswire.com/news/home/20250225398435/en/AI-Deepfake-Fraud-Calls-Dominate-Q4-Scams-Costing-Consumers-Millions>