ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

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

2025
Астана

УДК 001(06)
ББК 72я631
F96

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

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың 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 имолодыхученых 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

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

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 аі 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

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

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%)[1]
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 кампанияларының 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 **Arup** 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

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