



XҒТАР 14.35.07
Шолу мақаласы

<https://doi.org/10.32523/3080-1710-2025-152-3-126-144>

Студенттер арасында киберқауіпсіздік хабардарлығы: систематикалық әдеби шолу және prisma PRISMA әдісімен талдау

А.А. Амзеева*¹, А.Е. Жұмабаева²

¹Қорқыт Ата атындағы Қызылорда университеті, Қызылорда, Қазақстан

²Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан

(E-mail: ¹aruna_amzeeva@mail.ru, ²aziya_e@mail.ru)

Аңдатпа. Қазіргі таңда интернет қолданушылары, әсіресе студенттер, фишинг, жеке деректердің ұрлануы, әлеуметтік инженерия, зиянды бағдарламалар мен кибербуллинг сияқты қауіп-қатерлерге жиі тап болады. Осыған байланысты, олардың ақпараттық қауіпсіздікке деген көзқарасын зерттеу және тиімді оқыту әдістерін анықтау маңызды. Зерттеуде PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) әдісі қолданылып, 20 ғылыми мақала талданды. Барлық зерттеулер Scopus дерекқорынан алынған, бұл зерттеудің сенімділігі мен ғылыми негізділігін арттырады. Нәтижелер студенттердің киберқауіптерге қатысты білім деңгейінің әртүрлі екенін көрсетті. Студенттердің киберқауіпсіздік туралы хабардарлығын арттыру үшін ең жиі қолданылатын әдістер ретінде тренингтер, ойын арқылы оқыту (геймификация), интерактивті оқыту, сауалнама және тесттер, сондай-ақ мониторинг пен бақылау қарастырылды. Зерттеу нәтижелері студенттер арасында киберқауіпсіздік мәдениетін қалыптастыру үшін білім беру жүйесінде жаңа тәсілдерді енгізудің маңыздылығын көрсетеді. Әсіресе, интерактивті оқыту әдістері мен тәжірибелік сабақтар студенттердің ақпараттық қауіпсіздікке қатысты дағдыларын жақсартуға ықпал етеді. Бұл зерттеу студенттердің интернеттегі қауіпсіздігін арттыруға бағытталған тиімді стратегияларды анықтауға көмектеседі және білім беру саласында киберқауіпсіздікке қатысты әдістемелерді жетілдіруге негіз болады.

Түйін сөздер: киберқауіпсіздік, студенттер, PRISMA, жүйелі әдеби шолу, кибершабуылдар, ақпараттық қауіпсіздік.

Кіріспе

Интернетті жиі пайдаланатын адамдардың әртүрлі қауіп-қатерлерге тап болуы бүгінгі күннің өзекті мәселелерінің бірі. Бұл қауіп-қатерлер мен қауіпсіздік мәселелерін сипаттау үшін әртүрлі терминдер қолданылады, мысалы: "киберқауіпсіздік," "онлайн қауіпсіздік," "желідегі қауіпсіздік," және "интернет қауіпсіздігі." Көбіне бұл терминдер бір-бірінің орнына қолданылады, өйткені барлығы цифрлық ортадағы қауіпсіздікті

Түсті: 14.05.2025; Жөнделді: 26.08.2025; Мақұлданды: 29.09.2025; Онлайн қолжетімді: 30.09.2025

қамтамасыз етуге бағытталған. Киберқауіпсіздік – бұл кеңінен қолданылатын ұғым, бірақ оның нақты және жалпы қабылданған анықтамасы әлі де қалыптаспаған. Халықаралық телекоммуникациялар одағының (ITU) мәліметінше, киберқауіпсіздік – бұл онлайн орта мен пайдаланушы мәліметтерін қорғауға арналған ережелер, құралдар, оқыту жоспарлары, қауіпсіздік амалдары мен технологиялар жиынтығы. Қарапайым тілмен айтқанда, киберқауіпсіздік – адамдар мен түрлі мекемелерді интернеттегі қауіп-қатерлерден қорғау үшін қолданылатын әдістер мен шаралардың жиынтығы.

Қазіргі таңда студенттер уақыттарының айтарлықтай бөлігін интернетте өткізеді, бұл көбіне білім алу немесе қарым-қатынас жасау мақсатында жүзеге асады. Интернет үлкен мүмкіндіктер ашса да, онымен бірге түрлі қауіп-қатерлерді де алып келеді. Студенттер жас ерекшеліктері мен тәжірибесінің аздығына байланысты интернет пен цифрлық жүйелерді пайдаланудың пайдасы мен зиянын толық түсіне алмауы мүмкін. Олардың оқу мен жеке өмірі цифрлық технологияларға тәуелді болған сайын, бұл олардың жеке деректері мен қауіпсіздігіне уақыт өте келе елеулі әсер етуі мүмкін. Бұл жеке ақпараттың дұрыс қорғалмауы немесе дұрыс қолданылмауынан туындайтын мәселелерді қамтиды (Clemons and Wilson, 2015). Кейде адамдар бұл қауіптерді тек белгілі бір уақыт өткеннен кейін немесе қолайсыз жағдайға тап болғанда ғана түсінеді. Бұл оларды интернеттегі қысымға немесе шабуылға бейім етеді. Мұндай қауіптерді болдырмау үшін техникалық шаралар ғана жеткіліксіз. Интернет пайдаланушыларының киберқауіпсіздік туралы хабардар болуы және қауіптерді азайту бойынша белсенді әрекет етуі маңызды рөл атқарады. Қауіпсіздікті қамтамасыз ету әртүрлі факторларға тәуелді, бірақ негізгісі – қауіптерді түсініп, бағалай білу және оларды болдырмау үшін тиісті білімді дұрыс қолдана алу қабілеті. Бұл студенттердің интернеттегі қауіп-қатерлерден қорғау мәдениетін қалыптастыруда маңызды қадам болып табылады (Cumplings, Bergman and Kuznicki, 2014). Киберқауіпсіздік бойынша білім беру – бұл адамдарды киберқауіптер мен компьютерлер немесе мәліметтердің сол қауіптерге қалай ұшырайтыны туралы ақпараттандыруға арналған тәсіл. Бұл білім беру адамдарға ақпараттық қауіпсіздіктің маңыздылығын түсінуге және деректер мен желілерді қорғау үшін дұрыс шараларды қолданудың маңызын ұғынуға көмектеседі (Rahim *et al.*, 2015). Киберқауіпсіздік бойынша білім берудің басты екі мақсаты бар: біріншіден, адамдарды интернеттегі қауіп-қатерлер туралы ақпараттандыру, екіншіден, олардың бұл қауіптерді түсініп, қауіпсіздікке саналы түрде назар аударуын қамтамасыз ету. Адамдардың киберқауіпсіздік саласындағы білімін арттыру және олардың әлсіз тұстарын азайту жеке тұлға мен ұйым деңгейінде қауіпсіздікті нығайтуға көмектеседі. Сонымен қатар, киберқауіпсіздік және жеке ақпараттың құпиялылығы туралы хабардарлықты арттыру арқылы интернеттегі қауіпсіздік деңгейін айтарлықтай жақсартуға болады (Giannakas *et al.*, 2019). Киберқауіпсіздік туралы білім беру интернет пайдаланушыларын қорқыту немесе үрейлендіру үшін емес, керісінше, оларды киберқауіптерге қарсы әрекет етуге дайын болуға үйрету үшін қажет. Бұл бағдарлама, сонымен қатар, жаңа пайда болатын киберқауіптер туралы ақпаратпен бөлісудің маңызды алаңы болып табылады (Choo, 2011). Студенттердің киберқауіпсіздік туралы түсінігін дамыту – интернетті қауіпсіз әрі тиімді пайдалану үшін өте маңызды. Бұл студенттердің интернеттегі мінез-құлқын

жақсартып, цифрлық платформаларды дұрыс қолдануға көмектеседі. Бұл тақырыпқа академиктер мен практиктер ерекше назар аударғанын ескере отырып, студенттердің киберқауіпсіздігін қамтамасыз ету үшін қазіргі жағдайды жан-жақты талдау қажет. Мұндай талдау арқылы білім беру саласында ықтимал қауіп-қатерлер мен олқылықтарды анықтау, сонымен қатар киберқауіпсіздікке қатысты тиімді және тұрақты шешімдер қабылдауға ықпал ететін жағдайларды зерттеу маңызды. Қолданыстағы зерттеулерге шолу жасау болашақ зерттеулердің бағыттары мен нақты жоспарларын әзірлеуге де көмектеседі. Бұл шолу студенттердің киберқауіпсіздік туралы хабардарлығы бойынша зерттеулердің қазіргі жағдайын талдап, олардың алдында тұрған негізгі қауіптерді түсінуге және санасын арттыру үшін қолданылатын әртүрлі әдістерді зерттеуге бағытталған. Сонымен қатар, шолу барысында ұсынылған шешімдер мен әдістердің тиімділігі қарастырылып, олардың студенттердің цифрлық қауіпсіздігіне қалай әсер ететіндігіне баға беріледі. Осылайша, зерттеудің негізгі мақсаты – студенттердің киберқауіпсіздік тәуекелдерін азайтуға және олардың цифрлық ортада қауіпсіз болуына көмектесетін тиімді әдістерді анықтау.

Бұл зерттеудің негізгі мақсаты – студенттердің киберқауіпсіздік туралы хабардарлығын арттыру және олардың интернеттегі қауіп-қатерлерге қарсы қорғаныс дағдыларын дамыту үшін тиімді әдістерді анықтау. Сонымен қатар, зерттеу студенттердің киберқауіпсіздік саласындағы білім деңгейін бағалап, олардың интернетті қауіпсіз әрі саналы түрде пайдалануын қамтамасыз етуге бағытталған. Осы мақсатта киберқауіптерді түсіну, оларды болдырмау және киберқауіпсіздік мәдениетін қалыптастыруға арналған стратегиялар талданады.

Зерттеу міндеттері:

Киберқауіпсіздік ұғымын талдау – киберқауіпсіздік терминінің мазмұнын анықтау, оның негізгі компоненттері мен халықаралық ұйымдардағы анықтамаларын зерттеу.

Студенттердің интернетті пайдалану ерекшеліктерін анықтау – олардың желідегі негізгі белсенділігін, мақсаттарын және интернет қолдану уақытының көлемін сараптау.

Интернеттегі негізгі қауіп-қатерлерді жүйелеу – студенттер үшін аса өзекті қауіптерді (фишинг, мәліметтердің ұрлануы, кибербуллинг, зиянды бағдарламалар, әлеуметтік инженерия т.б.) анықтап, жіктеу.

Студенттердің киберқауіпсіздік туралы хабардарлығын бағалау – олардың цифрлық қауіпсіздік туралы білім деңгейін, негізгі қауіптерді тану және олардан қорғану дағдыларын зерттеу.

Киберқауіпсіздікті қамтамасыз ету әдістерін талдау – техникалық және білім беру шараларын қарастыру, студенттердің қауіпсіздік деңгейін арттыруға көмектесетін тәсілдерді анықтау. Киберқауіпсіздік туралы білім беру бағдарламаларын зерттеу – студенттер арасында киберқауіпсіздік мәдениетін қалыптастыруға арналған оқу-әдістемелік құралдар мен оқыту әдістерінің тиімділігін талдау.

Студенттердің интернеттегі қауіпсіздік мәдениетін дамыту жолдарын ұсыну – зерттеу нәтижелері негізінде киберқауіпсіздікке байланысты білім беру және ақпараттандыру бойынша нақты ұсыныстар әзірлеу.

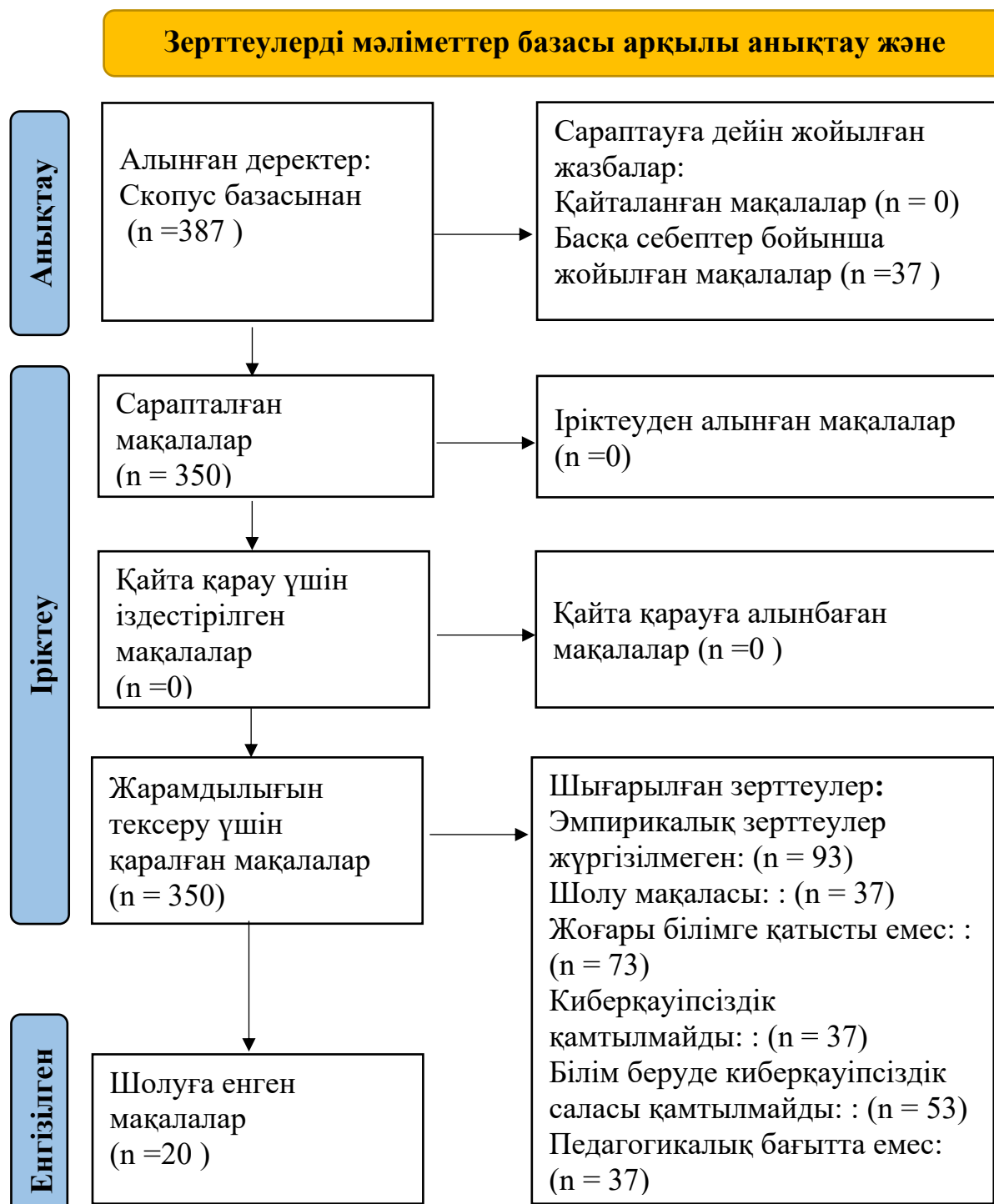
Осы зерттеу шеңберінде төмендегі зерттеу сұрақтары қарастырылды:

1. Қазіргі зерттеулерде студенттерге қатысты қандай киберқауіптер қарастырылады?
2. Студенттер арасында киберқауіпсіздік туралы хабардарлықты арттыру үшін қандай тәсілдер қолданылады?
3. Зерттеушілер студенттердің киберқауіпсіздік туралы хабардарлығын қалай бағалайды?

Материалдар мен әдістері

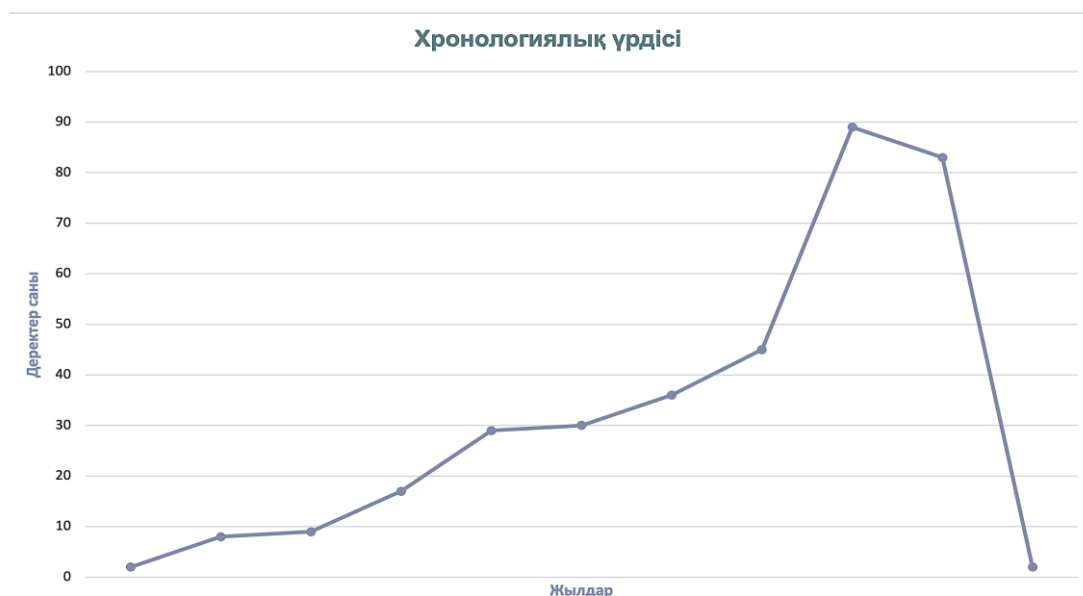
Бұл зерттеу Scopus мәліметтер базасынан алынған деректерді талдау негізінде құрылды. Зерттеу студенттердің киберқауіпсіздік туралы хабардарлығы тақырыбы бойынша жарияланған ғылыми жұмыстарды жүйелі түрде шолу және олардың негізгі бағыттарын айқындау. Scopus платформасындағы іздеу кезінде «студенттер және киберқауіпсіздік және хабардарлық» кілт сөздері енгізілді. Іздеу нәтижесінде 387 құжат табылды, олар мақалалар, конференция материалдары, кітаптар және басқа да жарияланымдар түрінде ұсынылған. Бұл іздеу студенттердің киберқауіпсіздік бойынша хабардарлығы туралы зерттеулерді жүйелі түрде талдауға бағытталған. Нәтижелер киберқауіпсіздік саласындағы білім беру мен хабардарлықты жақсарту үшін қолданылатын әдістер мен құралдарды зерттеуге мүмкіндік береді. Жарияланған құжаттар жыл бойынша сүзілді, ол 2015 жылдан 2025 жылға дейінгі диапазонды қамтылды, және соңғы 10 жыл таңдалған соң 350 құжат қалды. Келесі кезең құжаттарды сұрыптау нәтижелері бойынша мына құжат түрлері таңдалды: конференция материалдары 197 құжат, мақалалар 113 құжат, шолу мақалалары 23 құжат, кітаптар 20 құжат, кітап тараулары 18 құжат, шағын сауалнамалар мен шолулар 1 құжат. Бұл мәліметтер ғылыми ізденістердің кең спектрін қамтиды және киберқауіпсіздік саласындағы зерттеулерді түсіну үшін маңызды дереккөз болып табылады. Одан кейін зерттеулерді тек ағылшын тілінде қолжетімді құжаттармен шектедік. Жарияланымдар санының артуы графикте уақыт өткен сайын жарияланымдардың санының біртіндеп өскені байқалады, бұл тақырыптың өзектілігінің артуын көрсетеді. Осы зерттеуді басшылыққа алған үш негізгі зерттеу сұрағын шешу үшін PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) әдісі қолданылды. Бұл әдіс зерттеулерді жүйелі түрде іздеу, іріктеу, бағалау және талдау процесін кезең-кезеңімен сипаттайды. 1-кестеден көріп тұрғандай жалпы 350 мақала қалды, қайталанған жазбалар табылмады, себебі тек Scopus мәліметтер базасынан алынды. Іріктеу барысында жарамсыз деп табылған зерттеулер эмпирикалық зерттеулер жүргізілмеген зерттеулер, шолу мақаласы, жоғары білімге қатысы жоқ зерттеулер, білім беруде киберқауіпсіздік саласы қамтылмайтын және педагогикалық бағытта емес зерттеулер алынып тасталды. Барлық табылған деректерді қарап шығып, олардың тақырыптары мен тезистерін тексеріп, сәйкес келмейтіндерін алып тастап, осы жүйелі шолуға қатыстылығын анықтады. Аннотацияны зерделеу арқылы эмпирикалық зерттеу екендігі анықтала бермейді, сондықтан толық жұмыс оқылып шешім қабылданды. PRISMA әдісіне сәйкес Scopus дерекқорынан іріктелген 20 ғылыми мақала жүйелі әдеби шолу арқылы талданды.

Кесте 1. PRISMA 2020 жүйелі шолулар үшін арналған ағын диаграммасы (тек мәліметтер базалары мен тіркеу платформаларынан алынған іздеулер негізінде)



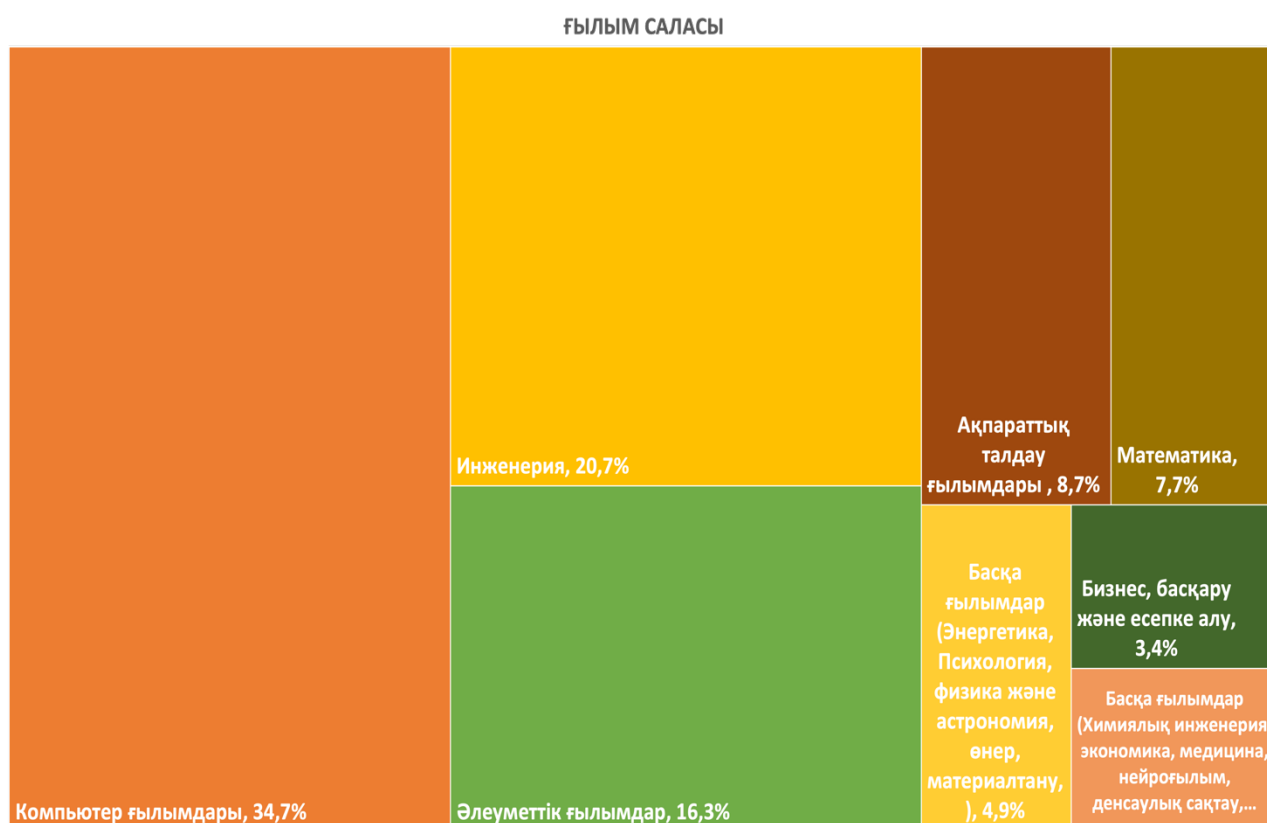
Нәтижелер мен талқылау

Соңғы жылдары (2015-2025) киберқауіпсіздік саласында ғылыми-зерттеу жұмыстарының айтарлықтай өсуі байқалды. 2023 және 2024 жылдары осы тақырыпқа арналған жарияланымдар санының едәуір артқаны көрінеді (1-сурет). Бұл салаға деген қызығушылықтың қазіргі жоғары деңгейі оның өзектілігі мен маңыздылығын айқындайды. Алайда, 2025 жылға жоспарланған ғылыми басылымдар әлі жарияланып үлгермегендіктен, бұл жылға қатысты толық мәлімет жоқ. Зерттеулер санының өсу қарқыны киберқауіпсіздік мәселелеріне ерекше назар аударылып жатқанын және бұл бағытта жүргізілетін зерттеулердің болашақта да өзекті болатынын көрсетеді.



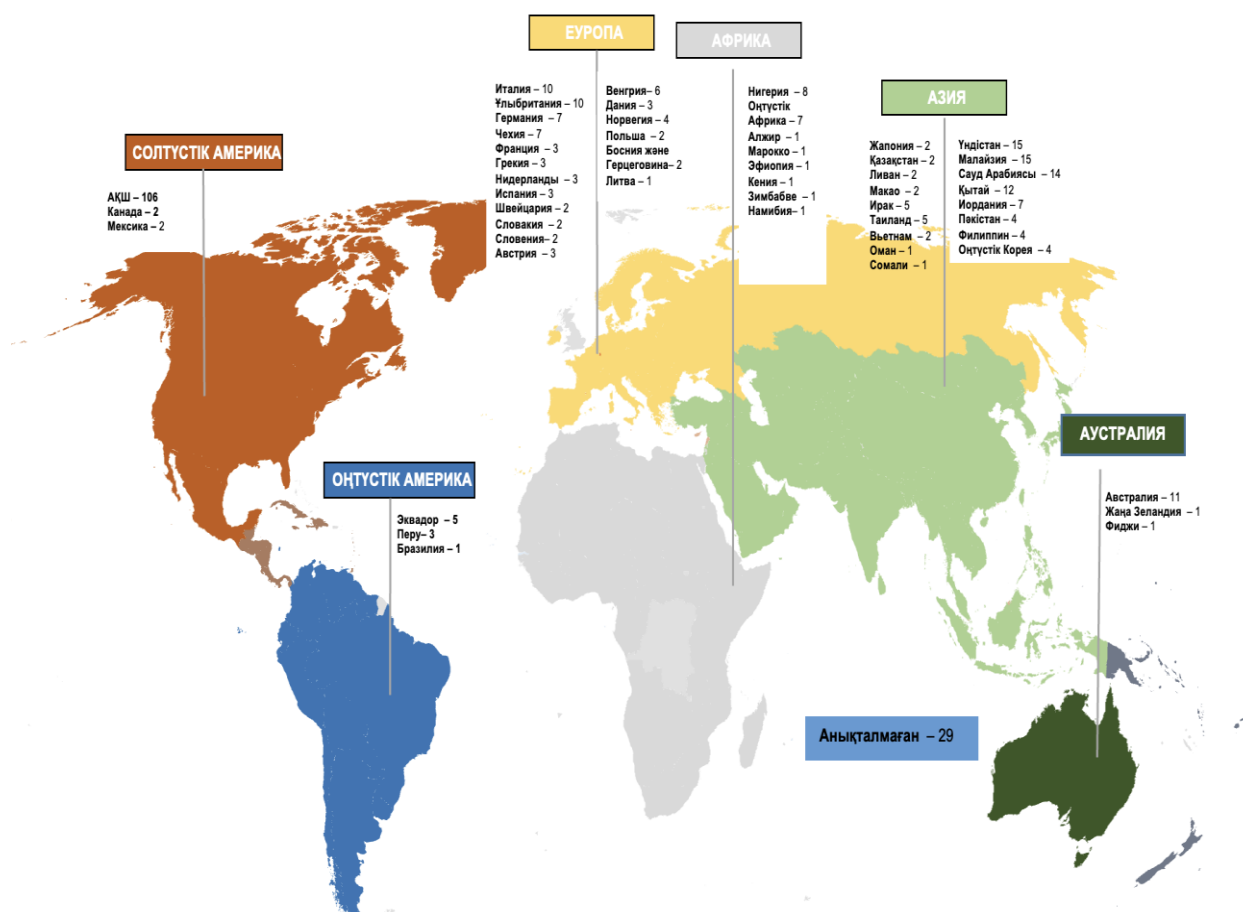
Сурет 1. Киберқауіпсіздік саласындағы ғылыми зерттеулердің жылдар бойынша динамикасы

Киберқауіпсіздік – компьютерлік және ақпараттық жүйелерді түрлі қауіп-қатерлерден қорғауға бағытталған сала. Бұл сала көпсалалы зерттеулерді қажет етеді, өйткені ақпараттық қауіпсіздік әртүрлі ғылыми бағыттарда маңызды рөл атқарады (2-сурет). Киберқауіпсіздік бойынша ең көп зерттеулер компьютер ғылымдарына (34,7%) тиесілі. Бұл бағытта желілік қауіпсіздік, деректерді шифрлау, зиянды бағдарламаларды анықтау, шабуылдарды алдын алу алгоритмдері зерттеледі. Инженерия ғылымдары (20,7%) өндірістік және инфрақұрылымдық жүйелердің қорғанысын қамтамасыз етуге бағытталған. Ақпараттық талдау ғылымдары (8,7%) кибершабуылдарды болжау, тәуекелдерді бағалау және басқару үшін қолданылады. Математика (7,7%) киберқауіпсіздіктің негізінде жатқан криптография, шифрлау алгоритмдері және күрделі есептеу әдістерін зерттеумен айналысады. Киберқауіпсіздік медицинада пациенттердің жеке деректерін қорғау, экономикада қаржы алаяқтығын анықтау, экологияда деректер қауіпсіздігін қамтамасыз ету сияқты көптеген салаларда қолданылады. Қазіргі таңда бұл сала қарқынды дамып келеді, себебі ақпараттық қауіпсіздік цифрлық технологиялардың дамуымен бірге жаңа қауіптерге бейімделуді талап етеді.



Сурет 2. Ғылыми зерттеулердің пәндік бағыттар бойынша үлесі

350 зерттеу әлемнің 72 елінде, алты құрлықты қамтиды. Алайда, бұл зерттеулердің таралуы құрлықтар арасында біркелкі болмаған. Солтүстік Америка – 77% . Құрлықтағы зерттеулердің 96%-дан астамы АҚШ-та жүргізілген, бұл АҚШ-тың зерттеу саласындағы басым рөлін көрсетеді. Азия зерттеулер саны бойынша екінші орында. Азия зерттеулердің 21%-ын қамтыған. Үндістан, Малайзия және Сауд Арабиясы көш бастап тұр. Еуропада 21 зерттеу жүргізілген, бұл жалпы зерттеулердің 15%-ын құрайды. Еуропада зерттеулер әртүрлі елдерде жүргізілгенімен, Италия мен Ұлыбритания ең көп үлеске ие. Оңтүстік Америка – 1%. Оңтүстік Америкада зерттеулер санының аздығы аймақтағы ғылыми жұмыстардың жеткіліксіздігін көрсетеді. Африка – 2%. Африкада зерттеу саны аз, зерттеулер негізінен Нигерия мен Оңтүстік Африкада жүргізілген. Аустралия (Океания) – 7%. Аймақтағы зерттеулердің 85%-ы Австралияның үлесінде. Зерттеулердің 29-ының географиялық аймағы көрсетілмеген. Киберқауіпсіздік саласындағы зерттеулердің таралуы көбіне дамыған елдерде шоғырланған. Азия мен Солтүстік Америка елдері көш бастап тұр, әсіресе АҚШ, Қытай және Малайзия осы саладағы жетекші зерттеу орталықтарына айналған. Ал киберқауіпсіздік қатері жаһандық сипатқа ие болғандықтан, Африка мен Оңтүстік Америка елдеріндегі ғылыми зерттеу жұмыстарын ынталандыру қажет (3-сурет).



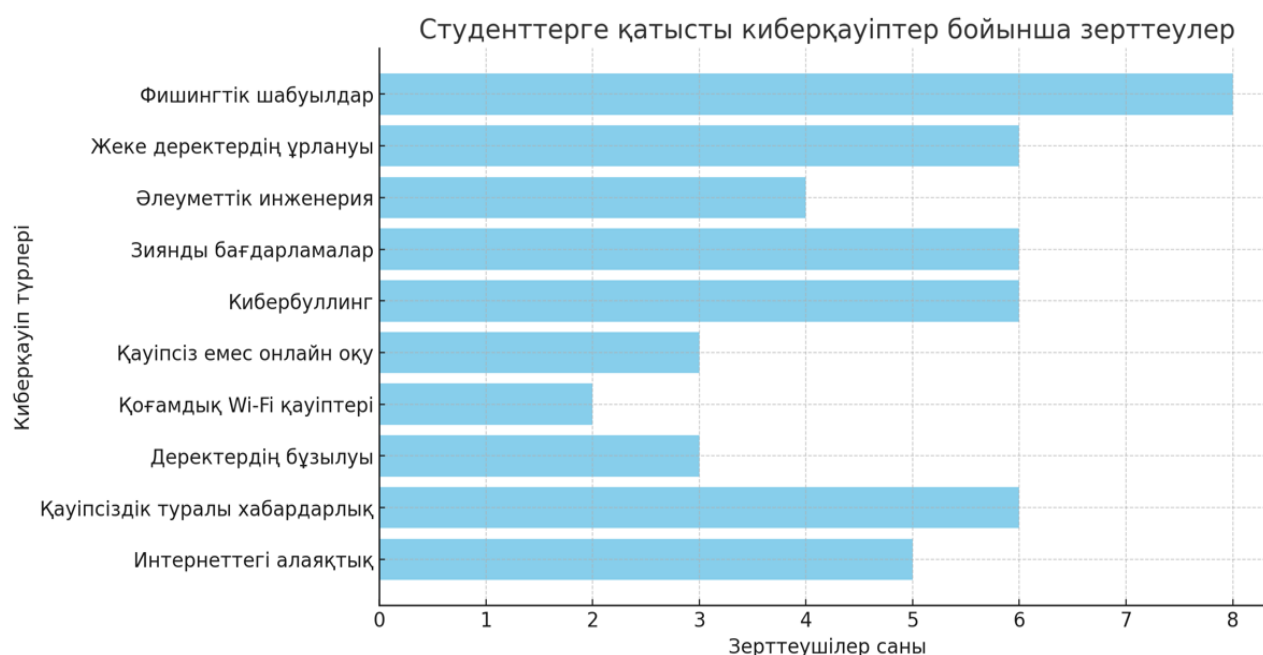
Сурет 3. Киберқауіпсіздік саласындағы зерттеулердің географиялық таралуы.

Зерттеудің негізгі сұрақтарына жауап беру мақсатында төменде әр сұраққа жеке-жеке талдау жасалды. Жауаптар қазіргі ғылыми әдебиеттерге сүйене отырып құрылып, студенттерге қатысты киберқауіптер мен олардан қорғану жолдарын анықтауға және хабардарлық деңгейін бағалау әдістеріне бағытталды.

1. Қазіргі зерттеулерде студенттерге қатысты қандай киберқауіптер қарастырылады?

Студенттердің киберқауіпсіздік хабардарлығы тақырыбы бойынша жарияланған ғылыми зерттеулерді талдау барысында, студенттерге қатысты ең кең тараған киберқауіптерді бірнеше негізгі санатқа бөлуге болады. Олардың ішінде ең бірінші орында фишингтік шабуылдар тұр. Бұл – алаяқтық хаттар немесе жалған веб-сайттар арқылы логин, құпиясөз сияқты жеке ақпаратты ұрлауға бағытталған әрекеттер. Әдетте фишинг қаржы институттарының тіркелгі деректерін ұрлаумен тең деп есептеледі, бірақ мұндай кибершабуылдар бірнеше ғалымдардың зерттеу мақалаларында көруге болады. (Senthilkumar and Easwaramoorthy, 2017; Peker, Ray and Da Silva, 2018; Aljohni *et al.*, 2021; Alqahtani, 2022, 2022; Erendor and Yildirim, 2022; Khamzina *et al.*, 2022; An *et al.*, 2023). Одан кейінгі маңызды қауіптердің бірі – жеке деректердің ұрлануы. Бұл

– студенттердің рұқсатсыз алынған жеке мәліметтерін заңсыз мақсатта пайдалану. Бұл фишингтік шабуылдар сияқты, жеке басын ұрлауда көптеген зерттеулерде студенттер үшін маңызды киберқауіп ретінде танылды. (Peker, Ray and Da Silva, 2018; Alharbi and Tassaddiq, 2021; Aljohni et al., 2021; Alqahtani, 2022; An et al., 2023; Huraj et al., 2023). *Әлеуметтік инженерия* да үлкен қауіптердің бірі ретінде қарастырылады. Бұл – адамдарды психологиялық манипуляция арқылы құпия ақпараттарды ашуға итермелейтін тактика. (Aljohni et al., 2021; Erendor and Yildirim, 2022; An et al., 2023; Alotibi, 2024). *Зиянды бағдарламалар* (вирустар, трояндар, шпиондық бағдарламалар) да студенттердің құрылғылары мен деректеріне қауіп төндіреді. (Peker, Ray and Da Silva, 2018; Aljohni et al., 2021; Alqahtani, 2022; Khamzina et al., 2022; An et al., 2023; Huraj et al., 2023). *Кибербуллинг*, яғни интернеттегі қорқыту және психологиялық қысым көрсету, студенттердің психологиялық саулығына әсер ететін маңызды қауіптердің бірі болып табылады. (Al-Janabi and Al-Shourbaji, 2016; Alqahtani, 2022; Garba, Siraj and Othman, 2022; Garcia and Bongo, 2022; Huraj et al., 2023). Сонымен қатар, *қауіпсіз емес онлайн оқу ортасы* да алаңдаушылық тудырады. Онлайн білім беру платформаларында қауіпсіздік шаралары жеткіліксіз болғандықтан, студенттердің жеке деректерінің бұзылуы немесе кибершабуылдарға ұшырау қаупі жоғары. (Peker, Ray and Da Silva, 2018; Erendor and Yildirim, 2022; An et al., 2023) *Қоғамдық Wi-Fi қауіптері* де елеулі проблема ретінде қарастырылады. Қорғалмаған желілерге қосылған кезде студенттердің мәліметтері киберқылмыскерлердің қолына түсуі мүмкін. (Huraj et al., 2023) Тағы бір маңызды мәселе – *деректердің бұзылуы*, яғни рұқсатсыз қол жеткізу арқылы жеке немесе құпия ақпараттың ашылуы. (Peker, Ray and Da Silva, 2018; the Universiti Kebangsaan Malaysia, Malaysia et al., 2020; Alharbi and Tassaddiq, 2021). Қауіпсіздік туралы жеткіліксіз хабардарлық студенттердің интернеттегі қауіптерге осалдығын арттырады. (Al-Janabi and Al-Shourbaji, 2016; Peker, Ray and Da Silva, 2018; An et al., 2023; Huraj et al., 2023; Morze et al., no date). Соңғы маңызды мәселе – *интернеттегі алаяқтық*, яғни жалған сайттар, жалған жарнамалар және басқа да қаржылық алаяқтық әрекеттер. (Senthilkumar and Easwaramoorthy, 2017; Garba, Siraj and Othman, 2022; Khamzina et al., 2022; Morze et al., no date). Жалпы алғанда, студенттер үшін киберқауіпсіздікті қамтамасыз ету өзекті мәселе болып табылады. Ғалымдардың зерттеулері бұл қауіптердің ауқымын түсінуге, олардан қорғанудың жолдарын дамытуға және киберқауіпсіздік туралы хабардарлықты арттыруға көмектеседі. Осы зерттеулерге сүйене отырып, студенттер үшін қауіпсіз интернет ортасын қалыптастыру шараларын күшейту қажеттілігі айқын көрінеді (4-сурет).

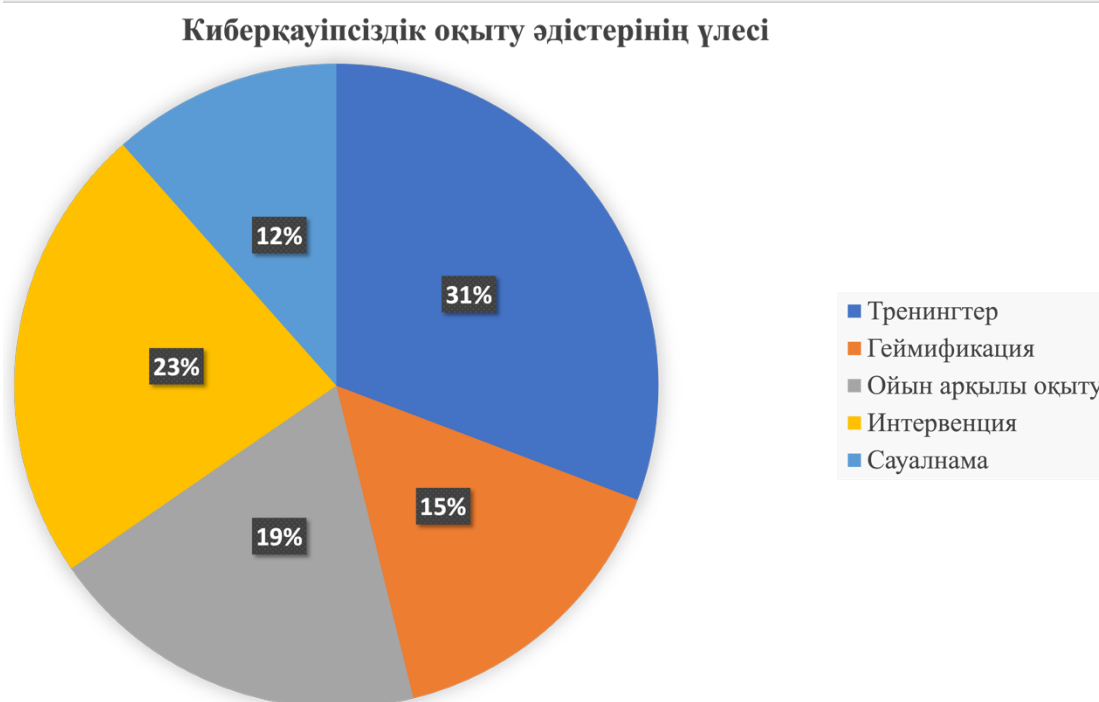


Сурет 4. Студенттерге қатысты киберқауіп түрлері бойынша зерттеулердің саны

2. Студенттер арасында киберқауіпсіздік туралы хабардарлықты арттыру үшін қандай тәсілдер қолданылады?

Ең жиі қолданылатын хабардар ету тәсілі тренингтер, ол жоғары оқу орындарында студенттердің киберқауіпсіздік туралы хабардарлығын арттыру мақсатында ұйымдас-тырылған. Бұл тренингтерде студенттерге фишингті тану, парольдерді қорғау, әлеуметтік желілердегі қауіпсіздік шараларын сақтау, деректерді шифрлау, ақпараттық жүйелердегі қауіптерден қорғану және зиянды әрекеттерден сақтану сияқты тақырыптар бойынша білім берілген. Тренингтердің негізгі бағыттары бірнеше маңызды кезеңдерден тұрады: алдымен, студенттерге әлеуметтік инженерия шабуылдарын анықтау және одан қорғану әдістері үйретілген. Одан кейін, әлеуметтік желілердегі қауіпсіздікті қамтамасыз ету үшін арнайы саясаттар мен нұсқаулықтар әзірленген. (the Universiti Kebangsaan Malaysia, Malaysia *et al.*, 2020; An *et al.*, 2023; Alotibi, 2024). Қауіпсіздік деңгейін арттыру мақсатында арнайы құралдар мен бағдарламалар қолданылып, оқу орындарында қауіпсіздік шаралары жетілдірілген. Соңғы кезеңде оқыту бағдарламасының тиімділігін тексеру үшін қауіпсіздік аудиттері жүргізілген. Бұл тренингтер барысында студенттерге фишингтік шабуылдарды анықтау, жүйелерді жаңарту, браузер қауіпсіздігін сақтау және VPN қолдану секілді практикалық дағдылар үйретілген. Сонымен қатар, киберқауіпсіздік тренингтері NIST Cybersecurity Framework негізінде арнайы дайындалған бағдарламаларға сүйенген (Garcia and Bongo, 2022). Бірнеше зерттеулерде тек қана студенттердің киберқауіпсіздік туралы базалық түсінігі жеткіліксіз болғаны анықталғанымен, киберқауіпсіздік хабардарлығын арттыру мақсатында әдістер жүргізілмеген. Киберқауіпсіздік бойынша тренингтер мен арнайы оқыту бағдарламаларын енгізу қажеттілігі ұсынылып қана қойған (Al-Janabi and Al-Shourbaji, 2016; Alharbi and Tassaddiq, 2021; Khan, Ikram and Saleem,

2024). Сонымен қатар, студенттерге ақпараттық сауаттылықты дамыту мақсатында арнайы «Primary Education» бағдарламасы ұсынылған. Практикалық әдістер ретінде лабораториялық сабақтар мен нақты өмірлік жағдайларда әрекет етуге арналған жаттығулар ұйымдастырылған. «Ақпараттық қауіпсіздік негіздері», «Педагогтарға арналған медиасауаттылық», «Педагогтарға арналған сыни ойлау» секілді ашық онлайн курстар (МООС) арқылы студенттер қосымша білім алған. Тәжірибелік жобалар аясында «Медиазнайко» және «Медиасауаттылық миссиясы» секілді ойындар қолданылып, студенттердің киберқауіпсіздікке қатысты машықтары дамытылған. Кейбір оқыту бағдарламалары бірнеше апта бойы өткізілген және студенттерге киберқауіптерден қорғану, жеке деректерді қорғау және заңдық аспектілер туралы кешенді білім беруге бағытталған (Khamzina *et al.*, 2022; Huraj *et al.*, 2023; Morze *et al.*,). Интерактивті оқыту барысында видеолар, интерактивті жаттығулар және ойын элементтері пайдаланылып, студенттердің оқу процесіне деген қызығушылығы арттырылды. Оқыту модульдері (мысалы, CSAM) студенттерге парольдерді қорғау, әлеуметтік инженерия шабуылдарынан қорғану, браузер қауіпсіздігі және мобильді құрылғыларды қорғау тақырыптарын қамтыған. (Peker, Ray and Da Silva, 2018). Зерттеу барысында көптеген студенттердің киберқауіпсіздік туралы білімі жеткіліксіз екені анықталды. Сондықтан, кибершабуылдардың алдын алу үшін тұрақты түрде киберқауіпсіздік бойынша оқыту бағдарламаларын мен практикалық жаттығуларды енгізу қажеттілігі ұсынылған. (Aljohni *et al.*, 2021; Alqahtani, 2022; Erendor and Yildirim, 2022; Garba, Siraj and Othman, 2022). Зерттеуде студенттердің киберқауіпсіздік туралы хабардарлығын арттыру үшін қолданылған негізгі әдістердің бірі – ойын арқылы оқыту және геймификация. Ойын арқылы оқыту әдісі студенттерге киберқауіпсіздікке қатысты білім беру процесінде ойындарды қолдануды қамтиды. Ойындар арқылы студенттер киберқауіптерді анықтауды, оларға қарсы әрекет етуді және қорғану жолдарын үйренген. Геймификация әдісі киберқауіпсіздік тақырыптары мен сұрақтарын ойын элементтері арқылы ұсынуды қамтиды. Оқу барысында студенттерге тапсырмаларды орындау, дұрыс жауап беру арқылы ұпай жинау және марапаттар алу мүмкіндігі берілген (Khader, Karam and Fares, 2021). Сонымен қатар, мақалада киберқауіпсіздікке қатысты білім беру үшін интервенция әдісі қолданылған. Интервенция барысында студенттерге арнайы онлайн тестілер мен интервенциялық бағдарламалар ұсынылған (Fadli *et al.*, 2024). Зерттеу барысында студенттердің киберқауіпсіздік туралы хабардарлығын бағалау үшін тек сауалнама әдісі ғана қолданылған мақалаларда кездесті (Senthilkumar and Easwaramoorthy, 2017; Alzahranı, 2021). Тек сауалнама арқылы студенттердің киберқауіптерді тану, олардан қорғану және дұрыс әрекет ету қабілеттерін шынайы түрде бағалау мүмкін емес (5-сурет).



Сурет 5. Студенттердің киберқауіпсіздік хабардарлығын арттыру әдістерінің қолданылу жиілігі

3. Зерттеушілер студенттердің киберқауіпсіздік туралы хабардарлығын қалай бағалайды?

Зерттеушілер студенттердің киберқауіпсіздік туралы хабардарлығын әртүрлі әдістер арқылы бағалайды (6-сурет). Олар арнайы әзірленген сауалнама сұрақтарын пайдалана отырып, студенттердің интернеттегі қауіпсіздік ережелерін қаншалықты білетінін және қауіпсіздікке қатысты күмәнді жағдайларда қандай әрекет жасайтынын анықтайды. (Aljohni *et al.*, 2021; Alqahtani, 2022; Garcia and Bongo, 2022; An *et al.*, 2023; Khan, Ikram and Saleem, 2024) Сонымен қатар, онлайн сауалнамалар арқылы студенттердің киберқауіпсіздікке қатысты көзқарасын, білімін және тәжірибесін жинайды. Бұл әдіс деректерді тез жинап, кең көлемде қатысушыларды қамтуға мүмкіндік береді, әрі зерт-теушілерге уақытты үнемдеуге көмектеседі (Al-Janabi and Al-Shourbaji, 2016; Senthilkumar and Easwaramoorthy, 2017; Erendor and Yildirim, 2022; Garba, Siraj and Othman, 2022; Morze *et al.*, no date). Кейбір зерттеушілер сандық зерттеу әдістемесін қолданады. Бұл әдіс арқылы студенттердің киберқауіпсіздікке қатысты білімі мен мінез-құлқы сандық деректер негізінде бағаланады. Статистикалық талдау жасалып, киберқауіпсіздік бойынша нақты әрі сенімді мәліметтер алынады (Alharbi and Tassaddiq, 2021; Alzahrani, 2021; Huraj *et al.*, 2023). Алдын-ала және кейінгі тестілеу сауалнамасы арқылы зерттеушілер студенттердің оқыту немесе тренингтен бұрынғы және кейінгі білім деңгейін салыстырады. Бұл әдісте тренинг немесе білім беру бағдарламасының тиімділігін анықтауға болады (Peker, Ray and Da Silva, 2018; Khader, Karam and Fares, 2021; Khamzina *et al.*, 2022). Зерттеушілер студенттердің киберқауіпсіздікке қатысты нақты білімін тексеру үшін тесттер мен квиздер қолданады, бұл студенттердің қауіпсіздік

шараларын қаншалықты дұрыс меңгергенін анықтайды. Кейбір зерттеушілер бақылау және мониторинг әдісін қолданады. Бұл әдіс студенттердің интернеттегі қауіпсіздік ережелерін қалай қолданатынын нақты уақыт режимінде бақылауға және олардың мінез-құлқын зерттеуге арналған (Fadli *et al.*, 2024). Сондай-ақ, зерттеушілер интервьюлар арқылы студенттердің киберқауіпсіздікке қатысты терең пікірлері мен тәжірибелерін анықтайды. Ашық сұрақтар арқылы алынған жауаптар киберқауіпсіздікке қатысты маңызды ақпарат жинауға және осы саладағы осал тұстарды анықтауға көмектеседі (Alotibi, 2024). Әрбір әдіс студенттердің киберқауіпсіздік туралы хабардарлығын жан-жақты бағалауға және олардың интернеттегі қауіпсіздігін арттыруға бағытталған тиімді қадамдар болып табылады.



Сурет 6. Киберқауіпсіздік саласындағы зерттеу әдістерінің классификациясы

Қорытынды

Қазіргі цифрлық дәуірде студенттердің киберқауіпсіздік туралы хабардарлығы білім беру саласындағы маңызды мәселелердің бірі болып табылады. Зерттеу барысында PRISMA әдісін қолдану арқылы Scopus мәліметтер базасынан алынған 20 ғылыми еңбектерге жүйелі шолу жасалды. Талдау нәтижелері студенттердің интернеттегі қауіп-қатерлерге қатысты хабардарлық деңгейінің әртүрлі екенін көрсетті. Зерттеу барысында студенттерге ең жиі кездесетін киберқауіптер анықталды. Олардың ішінде фишингтік шабуылдар, жеке деректердің ұрлануы, әлеуметтік инженерия, зиянды бағдарламалар және кибербуллинг ерекше орын алады. Сондай-ақ, қауіпсіз емес онлайн оқу ортасы, қоғамдық Wi-Fi-дың осалдығы, деректердің бұзылуы және интернеттегі алаяқтық студенттердің интернеттегі қауіпсіздігін айтарлықтай әлсірететін факторлар екені белгілі болды. Киберқауіпсіздік туралы хабардарлықты арттыру үшін ең тиімді әдістер ретінде тренингтер, ойын арқылы оқыту (геймификация), интерактивті оқыту, сауалнама және тесттер, сондай-ақ мониторинг пен бақылау тәсілдері қолданылғаны анықталды.

Тренингтер мен тәжірибелік сабақтар студенттердің ақпараттық қауіпсіздікке деген қызығушылығын арттырып, олардың практикалық дағдыларын нығайтуға көмектеседі. Зерттеушілер студенттердің киберқауіпсіздік туралы хабардарлығын бағалау үшін түрлі әдістерді қолданған. Олардың ішінде сауалнамалар, сандық зерттеу әдістері, алдын-ала және кейінгі тестілеу, бақылау және мониторинг, сондай-ақ интервью әдістері жиі кездеседі. Бұл тәсілдер студенттердің киберқауіпсіздікке қатысты білімін жан-жақты бағалап, олардың интернеттегі қауіпсіздікке деген көзқарасын тереңірек зерттеуге мүмкіндік береді. Жалпы, зерттеу нәтижелері студенттердің киберқауіпсіздік мәдениетін дамыту үшін білім беру жүйесінде жаңа тәсілдерді енгізудің маңыздылығын көрсетеді. Киберқауіпсіздік бойынша білім беруді жетілдіру, интерактивті оқыту әдістерін кеңінен қолдану және студенттердің қауіпсіздікке саналы түрде назар аударуын қамтамасыз ету – интернеттегі қауіп-қатерлерден қорғанудың негізгі қадамдары. Бұл зерттеу студенттердің интернеттегі қауіпсіздігін арттыруға бағытталған тиімді стратегияларды анықтауға көмектеседі және білім беру саласында киберқауіпсіздікке қатысты әдістемелерді жетілдіруге негіз болады. Киберқауіптермен күресу үшін студенттердің білімін жетілдіру, олардың саналы интернет пайдаланушылары болуына ықпал ету қазіргі заманғы білім беру жүйесінің басым бағыттарының бірі болуы тиіс.

Авторлардың үлесі

А.А. Амзеева – зерттеу тұжырымдамасын әзірлеп, оның негізгі бағыттарын анықтайды. Сондай-ақ, деректерді талдау жұмыстарын жүргізіп, зерттеу нәтижелерін интерпретациялады. Зерттеудің теориялық негіздемесін қалыптастыру мақсатында әдеби шолу жасап, қажетті материалдарды іріктеу мен жүйелеуге атсалысты. Сонымен қатар, қолданылған әдістемелерді жетілдіруге, олардың тиімділігін арттыруға назар аударды. Алынған нәтижелерді жан-жақты талқылап, оларды ғылыми тұрғыда негіздеу жұмыстарын жүргізді. Осы зерттеудің нәтижелерін жүйелеп, мақаланы жазу барысында негізгі құрылымын әзірлеп, мазмұндық сапасын арттыруға айтарлықтай үлес қосты.

А.Е. Жұмабаева – зерттеудің қорытынды бөлімін жазу барысында алынған нәтижелерді жинақтап, оларды ғылыми тұжырымдармен бекітті. Мақаланың соңғы нұсқасын әзірлеп, оның құрылымдық бірізділігін қамтамасыз етті. Сонымен қатар, мақаланы баспаға дайындау жұмыстарын жүргізіп, оның ғылыми стильге сәйкестігін қадағалап, редакциялық түзетулер енгізді.

Әдебиеттер тізімі:

Alharbi, T. and Tassaddiq, A. (2021) 'Assessment of Cybersecurity Awareness among Students of Majmaah University', *Big Data and Cognitive Computing*, 5(2), p. 23. Available at: <https://doi.org/10.3390/bdcc5020023>

Al-Janabi, S. and Al-Shourbaji, I. (2016) 'A Study of Cyber Security Awareness in Educational Environment in the Middle East', *Journal of Information & Knowledge Management*, 15(01), p. 1650007. Available at: <https://doi.org/10.1142/S0219649216500076>.

Aljohani, W. et al. (2021) 'Cybersecurity Awareness Level: The Case of Saudi Arabia University Students', *International Journal of Advanced Computer Science and Applications*, 12(3). Available at: <https://doi.org/10.14569/IJACSA.2021.0120334>.

Alotibi, G. (2024) 'A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks', *Engineering, Technology & Applied Science Research*, 14(2), pp. 13787–13795. Available at: <https://doi.org/10.48084/etasr.7123>.

Alqahtani, M.A. (2022) 'Factors Affecting Cybersecurity Awareness among University Students', *Applied Sciences*, 12(5), p. 2589. Available at: <https://doi.org/10.3390/app12052589>.

Alzahrani, L. (2021) 'Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes', *International Journal of Advanced Computer Science and Applications*, 12(11). Available at: <https://doi.org/10.14569/IJACSA.2021.0121172>.

An, Q. et al. (2023) 'How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates', *International Journal of Information Security*, 22(2), pp. 305–317. Available at: <https://doi.org/10.1007/s10207-022-00637-z>.

Choo, K.-K.R. (2011) 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, 30(8), pp. 719–731. Available at: <https://doi.org/10.1016/j.cose.2011.08.004>.

Clemons, E. and Wilson, J. (2015) 'Family Preferences Concerning Online Privacy, Data Mining, and Targeted Ads: Regulatory Implications', *Journal of Management Information Systems*, 32, pp. 40–70. Available at: <https://doi.org/10.1080/07421222.2015.1063277>.

Cummings, E.M., Bergman, K.N. and Kuznicki, K.A. (2014) 'Emerging Methods for Studying Families as Systems', in S.M. McHale, P. Amato, and A. Booth (eds) *Emerging Methods in Family Research*. Cham: Springer International Publishing (National Symposium on Family Issues), pp. 95–108. Available at: https://doi.org/10.1007/978-3-319-01562-0_6.

Erendor, M.E. and Yildirim, M. (2022) 'Cybersecurity Awareness in Online Education: A Case Study Analysis', *IEEE Access*, 10, pp. 52319–52335. Available at: <https://doi.org/10.1109/ACCESS.2022.3171829>.

Fadli, R. et al. (2024) 'Assessing Cybersecurity Awareness Among Vocational Students in Office Administration', *International Journal of Safety and Security Engineering*, 14(4), pp. 1115–1123. Available at: <https://doi.org/10.18280/ijssse.140410>.

Garba, A.A., Siraj, M.M. and Othman, S.H. (2022) 'An assessment of cybersecurity awareness level among Northeastern University students in Nigeria', *International Journal of Electrical and Computer Engineering (IJECE)*, 12(1), p. 572. Available at: <https://doi.org/10.11591/ijece.v12i1.pp572-584>.

Garcia, A.B. and Bongo, S.M.C. (2022) 'A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education', in 2022 8th International Conference on Information Management (ICIM). 2022 8th International Conference on Information Management (ICIM), Cambridge, United Kingdom: IEEE, pp. 116–119. Available at: <https://doi.org/10.1109/ICIM56520.2022.00028>.

Giannakas, F. et al. (2019) 'A comprehensive cybersecurity learning platform for elementary education', *Information Security Journal: A Global Perspective*, 28(3), pp. 81–106. Available at: <https://doi.org/10.1080/19393555.2019.1657527>.

Huraj, L. et al. (2023) 'Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students', *TEM Journal*, pp. 623–633. Available at: <https://doi.org/10.18421/TEM122-05>.

Khader, M., Karam, M. and Fares, H. (2021) 'Cybersecurity Awareness Framework for Academia', *Information*, 12(10), p. 417. Available at: <https://doi.org/10.3390/info12100417>.

Khamzina, B. et al. (2022) 'Determination of Cyber Security Issues and Awareness Training for University Students', *International Journal of Emerging Technologies in Learning (ijET)*, 17(18), pp. 177–190. Available at: <https://doi.org/10.3991/ijet.v17i18.32193>.

Khan, N.F., Ikram, N. and Saleem, S. (2024) 'Effects of socioeconomic and digital inequalities on cybersecurity in a developing country', *Security Journal*, 37(2), pp. 214–244. Available at: <https://doi.org/10.1057/s41284-023-00375-4>.

Morze, N. et al. (no date) 'Formation of Internet Resources Critical Evaluation Skills of Future Primary School Teachers'.

Peker, Y., Ray, L. and Da Silva, S. (2018) 'Online Cybersecurity Awareness Modules for College and High School Students', in 2018 National Cyber Summit (NCS). 2018 National Cyber Summit (NCS), Huntsville, AL: IEEE, pp. 24–33. Available at: <https://doi.org/10.1109/NCS.2018.00009>.

Rahim, N.H.A. et al. (2015) 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes*, 44(4), pp. 606–622. Available at: <https://doi.org/10.1108/K-12-2014-0283>.

Senthilkumar, K. and Easwaramoorthy, S. (2017) 'A Survey on Cyber Security awareness among college students in Tamil Nadu', *IOP Conference Series: Materials Science and Engineering*, 263, p. 042043. Available at: <https://doi.org/10.1088/1757-899X/263/4/042043>.

the Universiti Kebangsaan Malaysia, Malaysia et al. (2020) 'The Importance of Cybersecurity Education in School', *International Journal of Information and Education Technology*, 10(5), pp. 378–382. Available at: <https://doi.org/10.18178/ijiet.2020.10.5.1393>.

А.А. Амзеева¹, А.Е. Жумабаева²

¹*Кызылординский университет имени Коркыт Ата, Кызылорда, Казахстан*

²*Казахский национальный педагогический университет имени Абая, Алматы, Казахстан*

Осведомленность студентов о кибербезопасности: систематический обзор литературы и анализ методом PRISMA

Аннотация. В настоящее время пользователи интернета, особенно студенты, часто сталкиваются с такими угрозами, как фишинг, кража личных данных, социальная инженерия, вредоносные программы и кибербуллинг. В связи с этим важно изучить их отношение к информационной безопасности и определить эффективные методы обучения. В данном исследовании применяется метод PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), в рамках которого были проанализированы 20 научных статей. Все исследования были отобраны из базы данных Scopus, что повышает надежность и научную обоснованность данного обзора. Результаты показали различный уровень знаний студентов о киберугрозах. Наиболее распространенными методами повышения осведомленности студентов о кибербезопасности являются тренинги, обучение через игры (геймификация), интерактивное обучение, опросы и тестирование, а также мониторинг и контроль. Результаты исследования подтверждают необходимость внедрения новых подходов в образовательную систему для формирования культуры кибербезопасности среди студентов. Особенно эффективными оказались интерактивные методы обучения и практические занятия, способствующие развитию у студентов навыков информационной безопасности. Данное исследование помогает определить эффективные стратегии повышения безопасности студентов в интернете и закладывает основу для совершенствования методик преподавания кибербезопасности в образовательной сфере.

Ключевые слова: кибербезопасность, студенты, PRISMA, систематический обзор литературы, кибератаки, информационная безопасность.

A.A. Amzeyeva¹, A.E. Zhumabayeva²

¹Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan

²Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

Cybersecurity Awareness Among Students: A Systematic Literature Review and PRISMA-Based Analysis

Abstract. Nowadays, internet users, especially students, frequently encounter threats such as phishing, identity theft, social engineering, malware, and cyberbullying. In this regard, it is crucial to investigate their cybersecurity awareness and identify effective teaching methods. This study employs the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method, analyzing 20 scientific articles. All studies were sourced from the Scopus database, ensuring this review's reliability and scientific validity. The results indicate varying levels of cybersecurity knowledge among students. The most commonly used methods to enhance students' cybersecurity awareness include training sessions, game-based learning (gamification), interactive learning, surveys and tests, as well as monitoring and supervision. The study highlights the importance of integrating new approaches into the education system to foster a cybersecurity culture among students. Interactive teaching methods and practical lessons have proven to be particularly effective in improving students' information security skills. This research contributes to the identification of effective strategies for enhancing students' online security and serves as a foundation for improving cybersecurity education methodologies in the academic field.

Keywords: cybersecurity, students, PRISMA, systematic literature review, cyberattacks, information security.

References:

Alharbi, T. and Tassaddiq, A. (2021) 'Assessment of Cybersecurity Awareness among Students of Majmaah University', *Big Data and Cognitive Computing*, 5(2), p. 23. Available at: <https://doi.org/10.3390/bdcc5020023>.

Al-Janabi, S. and Al-Shourbaji, I. (2016) 'A Study of Cyber Security Awareness in Educational Environment in the Middle East', *Journal of Information & Knowledge Management*, 15(01), p. 1650007. Available at: <https://doi.org/10.1142/S0219649216500076>.

Aljohni, W. et al. (2021) 'Cybersecurity Awareness Level: The Case of Saudi Arabia University Students', *International Journal of Advanced Computer Science and Applications*, 12(3). Available at: <https://doi.org/10.14569/IJACSA.2021.0120334>.

Alotibi, G. (2024) 'A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks', *Engineering, Technology & Applied Science Research*, 14(2), pp. 13787–13795. Available at: <https://doi.org/10.48084/etasr.7123>.

Alqahtani, M.A. (2022) 'Factors Affecting Cybersecurity Awareness among University Students', *Applied Sciences*, 12(5), p. 2589. Available at: <https://doi.org/10.3390/app12052589>.

Alzahrani, L. (2021) 'Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes', *International Journal of Advanced Computer Science and Applications*, 12(11). Available at: <https://doi.org/10.14569/IJACSA.2021.0121172>.

An, Q. et al. (2023) 'How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates', *International Journal of Information Security*, 22(2), pp. 305–317. Available at: <https://doi.org/10.1007/s10207-022-00637-z>.

- Choo, K.-K.R. (2011) 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, 30(8), pp. 719–731. Available at: <https://doi.org/10.1016/j.cose.2011.08.004>.
- Clemons, E. and Wilson, J. (2015) 'Family Preferences Concerning Online Privacy, Data Mining, and Targeted Ads: Regulatory Implications', *Journal of Management Information Systems*, 32, pp. 40–70. Available at: <https://doi.org/10.1080/07421222.2015.1063277>.
- Cummings, E.M., Bergman, K.N. and Kuznicki, K.A. (2014) 'Emerging Methods for Studying Families as Systems', in S.M. McHale, P. Amato, and A. Booth (eds) *Emerging Methods in Family Research*. Cham: Springer International Publishing (National Symposium on Family Issues), pp. 95–108. Available at: https://doi.org/10.1007/978-3-319-01562-0_6.
- Erendor, M.E. and Yildirim, M. (2022) 'Cybersecurity Awareness in Online Education: A Case Study Analysis', *IEEE Access*, 10, pp. 52319–52335. Available at: <https://doi.org/10.1109/ACCESS.2022.3171829>.
- Fadli, R. et al. (2024) 'Assessing Cybersecurity Awareness Among Vocational Students in Office Administration', *International Journal of Safety and Security Engineering*, 14(4), pp. 1115–1123. Available at: <https://doi.org/10.18280/ijssse.140410>.
- Garba, A.A., Siraj, M.M. and Othman, S.H. (2022) 'An assessment of cybersecurity awareness level among Northeastern University students in Nigeria', *International Journal of Electrical and Computer Engineering (IJECE)*, 12(1), p. 572. Available at: <https://doi.org/10.11591/ijece.v12i1.pp572-584>.
- Garcia, A.B. and Bongo, S.M.C. (2022) 'A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education', in 2022 8th International Conference on Information Management (ICIM). 2022 8th International Conference on Information Management (ICIM), Cambridge, United Kingdom: IEEE, pp. 116–119. Available at: <https://doi.org/10.1109/ICIM56520.2022.00028>.
- Giannakas, F. et al. (2019) 'A comprehensive cybersecurity learning platform for elementary education', *Information Security Journal: A Global Perspective*, 28(3), pp. 81–106. Available at: <https://doi.org/10.1080/19393555.2019.1657527>.
- Huraj, L. et al. (2023) 'Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students', *TEM Journal*, pp. 623–633. Available at: <https://doi.org/10.18421/TEM122-05>.
- Khader, M., Karam, M. and Fares, H. (2021) 'Cybersecurity Awareness Framework for Academia', *Information*, 12(10), p. 417. Available at: <https://doi.org/10.3390/info12100417>.
- Khamzina, B. et al. (2022) 'Determination of Cyber Security Issues and Awareness Training for University Students', *International Journal of Emerging Technologies in Learning (iJET)*, 17(18), pp. 177–190. Available at: <https://doi.org/10.3991/ijet.v17i18.32193>.
- Khan, N.F., Ikram, N. and Saleem, S. (2024) 'Effects of socioeconomic and digital inequalities on cybersecurity in a developing country', *Security Journal*, 37(2), pp. 214–244. Available at: <https://doi.org/10.1057/s41284-023-00375-4>.
- Morze, N. et al. (no date) 'Formation of Internet Resources Critical Evaluation Skills of Future Primary School Teachers'.
- Peker, Y., Ray, L. and Da Silva, S. (2018) 'Online Cybersecurity Awareness Modules for College and High School Students', in 2018 National Cyber Summit (NCS). 2018 National Cyber Summit (NCS), Huntsville, AL: IEEE, pp. 24–33. Available at: <https://doi.org/10.1109/NCS.2018.00009>.
- Rahim, N.H.A. et al. (2015) 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes*, 44(4), pp. 606–622. Available at: <https://doi.org/10.1108/K-12-2014-0283>.

Senthilkumar, K. and Easwaramoorthy, S. (2017) 'A Survey on Cyber Security awareness among college students in Tamil Nadu', IOP Conference Series: Materials Science and Engineering, 263, p. 042043. Available at: <https://doi.org/10.1088/1757-899X/263/4/042043>.

the Universiti Kebangsaan Malaysia, Malaysia et al. (2020) 'The Importance of Cybersecurity Education in School', International Journal of Information and Education Technology, 10(5), pp. 378–382. Available at: <https://doi.org/10.18178/ijiet.2020.10.5.1393>.

Авторлар туралы мәліметтер:

Амзеева А.А. – жауапты автор, «Бастауыш оқыту педагогикасы мен әдістемесі» білім беру бағдарламасының докторанты, Қорқыт Ата атындағы Қызылорда университеті, 120014, Қызылорда қ., Қазақстан Республикасы.

Жұмабаева Ә.Е. – педагогика ғылымдарының докторы, Абай атындағы Қазақ ұлттық педагогикалық университетінің «Бастауыш білім беру» кафедрасының профессоры, 050010, Алматы қ., Қазақстан Республикасы.

Сведения об авторах:

Амзеева А.А. – автор для корреспонденции, докторант образовательной программы «Педагогика и методика начального обучения», Кызылординский университет имени Коркыт Ата, 120014, г. Кызылорда, Республика Казахстан.

Жұмабаева А.Е. – доктор педагогических наук, профессор кафедры «Начальное образование» Казахского национального педагогического университета имени Абая, 050010, г. Алматы, Республика Казахстан.

Information about authors:

Amzeeva A.A. – Corresponding author, PhD student of the educational program "Pedagogy and Methods of Primary Education," Korkyt Ata Kyzylorda University, 120014, Kyzylorda, Republic of Kazakhstan.

Zhumabayeva A.E. – Doctor of Pedagogical Sciences, Professor of the "Primary Education" Department, Abai Kazakh National Pedagogical University, 050010, Almaty, Republic of Kazakhstan.