КОДТЫҢ ТҮПНҰСҚАСЫ АШЫҚ ТҮРДЕГІ MFA ШЕШІМДЕРІНЕ АНАЛИЗ ЖАСАУ

Ж.М. Алимжанова[1], Н.Ж. Тойбек[2], А.К. Али[3], Н.М. Ниязбек[4]
[1,2,3,4] Әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан
e-mail: nurtas.toibek@gmail.com
[2]ORCID ID: https://orcid.org/0009-0002-2180-0317
[3]ORCID ID: https://orcid.org/0009-0006-2165-0960
[4]ORCID ID: https://orcid.org/0009-0006-6105-6229

Аңдатпа. Бұл мақала ең жақсы 5 ашық бастапқы MFA шешімдеріне арналған. Технология тез өзгеруде, сондықтан бізге ашық бастапқы MFA шешімдерін бейімдеу қажет болады. Көп факторлы аутентификация (MFA) — бұл пайдаланушының жеке басын тексеру үшін қолданылатын Әдіс пен технология. Пайдаланушыларға кіру немесе транзакция жасау үшін тіркелгі деректері санаттарының кем дегенде екі немесе одан да көп түрі қажет. Кем дегенде екі тӘуелсіз тіркелгі деректерінің сәтті үйлесімі MFA әдісінің міндетті талабы болып табылады. Ол Әдетте тіркелгі деректерінің келесі үш санатының бірін біріктіреді:

1. Пайдаланушы не біледі: құпия сөз немесе Код фразасы
2. Адамда не бар: қауіпсіздік белгісі, салпыншақ немесе SIM картасы
3. Пайдаланушы нені білдіреді: саусақ іздері, торлы қабық немесе ирис, дауыс немесе бетті тану сияқты биометриялық деректер.

MFA пайдаланушыдан ресурсқа қол жеткізу үшін екі немесе одан да көп тексеру факторларын ұсынуды талап етеді, мысалы, қолданба немесе онлайн тіркелгі. MFA логин мен парольге қосымша бір немесе бірнеше қосымша тексеру критерийлерін қажет етеді, бұл сәтті кибершабуылдың ықтималдығын азайтады. Жалпыға қол жетімді код "ашық бастапқы код"болып саналады. Сонымен қатар, ашық бастапқы құралдар мен шешімдер қауіпсіз, өйткені кодты кез-келген адам тексеріп, тексере алады.

Кілттік сөздер: MFA, 2FA, LDAP, AAA, RADIUS, оқиғаларды аутентификациялау және есепке алу жүйесі, көп факторлы аутентификация, ашық бастапқы шешім.

ANALYSIS OF OPEN SOURCE MFA SOLUTIONS

J.M. Alımjanova [1], N.J. Toıbek [2], A.K. Alı [3], N.M. Nıazbek[4]
[1,2,3,4]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
e-mail: nurtas.toibek@gmail.com
[2]ORCID ID: https://orcid.org/0009-0002-2180-0317
[3]ORCID ID: https://orcid.org/0009-0006-2165-0960
[4]ORCID ID: https://orcid.org/0009-0006-6105-6229

Abstract. This article is devoted to the top 5 open source MFA solutions. Technology is changing rapidly, so we will need to adapt open source MFA solutions. Multi-factor authentication (MFA) is a method and technology used to verify the identity of a user. Users need at least two or more types of credential categories to log in or make transactions. A successful combination of at least two independent credentials is a mandatory requirement for the MFA method. It usually combines one of the following three categories of credentials:

1. What the user knows: password or code phrase
2. What does a person have: security badge, keychain or SIM card
3.What the user means: biometric data such as fingerprints, retina or iris, voice or face recognition.

MFA requires the user to provide two or more verification factors to access a resource, such as an app or an online account. MFA requires one or more additional verification criteria in addition to the login and password, which reduces the likelihood of a successful cyber attack. Public code is considered"open source". In addition, open source tools and solutions are safe because the code can be tested and verified by anyone.

Keywords: MFA, 2FA, LDAP, AAA, RADIUS, event authentication and accounting system, multi-factor authentication, open source solution.

Авторлар жайында мәлімет:

Қаз: Алимжанова Жанна Муратбековна – Әл-Фараби атындағы Қазақ Ұлттық Университетінің аға оқутышысы, физика-математика ғылымдарының кандидаты

Рус: Алимжанова Жанна Муратбековна – старший преподаватель Казахского национального университета имени Аль-Фараби, кандидат физико-математических наук

Англ: Alimzhanova Zhanna Muratbekovna - Senior Lecturer of Al-Farabi Kazakh National University, Candidate of Physical and Mathematical Sciences

Қаз: Тойбек Нұртас ЖӘнібекұлы - Әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, nurtas.toibek@gmail.com

Рус: Тойбек Нуртас Жанибекулы – магистрант Казахского национального университета имени аль-Фараби, nurtas.toibek@gmail.com

Англ: Toybek Nurtas Zhanibekuly – graduate student of Al-Farabi Kazakh National University, nurtas.toibek@gmail.com

Қаз: Әли Алтынай Қуанышқызы - Әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, alievaaltynai28@gmail.com

Рус: Али Алтынай Куанышкызы– магистрант Казахского национального университета имени аль-Фараби, alievaaltynai28@gmail.com

Англ: Ali Altynai Kuanyshqyzy – graduate student of Al-Farabi Kazakh National University, alievaaltynai28@gmail.com

Қаз: Ниязбек Нұрай Мейірханқызы - Әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, nurayniyazbek@gmail.com

Рус: Ниязбек Нурай Меирханкызы – магистрант Казахского национального университета имени аль-Фараби, nurayniyazbek@gmail.com

Англ: Niyazbek Nurai Meirkhanqyzy – graduate student of Al-Farabi Kazakh National University, nurayniyazbek@gmail.com

ӘОЖ 007.621.391

БОЛАШАҚ ИНФОРМАТИКА МҰҒАЛІМДЕРІН КИБЕРҚАУІПСІЗДІК БОЙЫНША КӘСІБИ ҚҰЗЫРЕТТІЛІКТЕРДІ ҚАЛЫПТАСТЫРУҒА ДАЙЫНДАУДЫҢ ӘДІСТЕМЕЛІК НЕГІЗДЕРІ

Мекебаев Н.О[1]., НазкеноваБ.Б[1]., Чайко Е.В[2].
[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[2]Рига техникалық университеті, Латвия, Рига
nurbapa@mail.ru, nazkenova_bayan@mail.ru, jelena.caiko@gmail.com
ORCID:0000-0002-9117-4369
ORCID: 0000-0002-6671-7835
ORCID: 0000-0002-1207-1418

Аңдатпа. Ақпараттық қауіпсіздік қоғамның ғаламдық Интернет желісіне тәуелділігінің артуына байланысты жаһандық проблема болып табылады, ал киберқауіптер экономика мен ұлттық қауіпсіздік үшін ең маңызды сын-қатерлердің бірі. Ақпараттық қауіпсіздік ұлттық басымдыққа айналды. Барлық ұйымдарға, соның ішінде Цифрлық компьютерлік технологиялармен жұмыс істейтін білім беру мекемелеріне киберқауіптердің динамикалық ортасында кибершабуылдармен күресу үшін мінез-құлық, басқару және техникалық білімді қамтитын құзыреттері мен дағдылары бар мамандар қажет. Осыған байланысты білікті мамандарға ғана емес, сонымен қатар мектеп орындығынан киберқауіпсіздік негіздерін үйрете алатын ақпараттық қауіпсіздік құзыреті бар мұғалімдерге де сұраныс артып келеді.

Кибершабуылдарға осал цифрлық технологияларды кеңінен қолдану мен ақпараттық қауіпсіздікті оқыту үшін білім беру процесін пайдаланудың жеткіліксіздігі, сондай-ақ ақпараттық қауіпсіздік бойынша информатика мұғалімдерін даярлауға сұраныстың артуы мен университеттің профессорлық-педагогикалық құрамының тиісті мамандарды даярлауға жеткіліксіз дайындығы арасындағы қайшылықтар ғылыми зерттеудің өзекті мәселесін тұжырымдауға мүмкіндік береді, бұл болашақ информатика мұғалімдерін даярлауды жүйелі түрде қамтамасыз ету және олардың ақпараттық қоғамды дамытудың қазіргі жағдайында ақпараттық қауіпсіздік бойынша кәсіби құзыреттерін қалыптастыру қажеттілігінен тұрады. Зерттеудің жаңалығы болашақ информатика мұғалімдеріне киберқауіпсіздік негіздерін үйрету және білім беруді цифрландыру жағдайында олардың ақпараттық қауіпсіздік құзыреттерін қалыптастыру тәсілін әзірлеуден тұрады.

Кілттік сөздер: информатика мұғалімі, ақпараттық қауіпсіздік, киберқауіпсіздік, кәсіби дайындық, құзыреттілік.

Кіріспе

Цифрлық білім беру жүйелерінде болашақ информатика мұғалімдерін даярлау заманауи технологияларды игеруді қамтиды [3; 4], бірақ мұғалімдерді даярлау бағдарламалары әдетте информатика мұғалімдерінің құзыреттілігін ақпараттық-коммуникациялық технологияларды игеру тұрғысынан қарастырады және ақпараттық қауіпсіздік бойынша мұғалімдерді даярлауға қатысты. Киберқауіпсіздік мүлдем қарастырылмайды, өйткені киберқауіпсіздік пен ақпараттық қауіпсіздік толығымен бірдей және синоним болып табылады [8]. Шетелде Еуропа елдерінде киберқауіпсіздік ақпараттық қауіпсіздіктен [21] бөлек салаға бөлініп, Қазақстанда біртіндеп енгізілуде.

Киберқауіпсіздік жаңа нәрсе емес және жиырма жылға жуық уақыт бойы Үкіметте, өнеркәсіпте және ғылыми ортада маңызды пікірталастардың тақырыбы болды [22]. Дегенмен, киберқауіпсіздікті анықтау мен қолдану саласында әртүрлі авторлар арасындағы келіспеушіліктердің себебі болған кейбір айырмашылықтар бар [7; 10]. Кейбір сарапшылар бұл тақырып қорқыныштың күшеюіне байланысты шамадан тыс және жасанды түрде ісінген деп мәлімдейді, ал «кибер соғыс» сияқты термин ұтымды емес, эмоционалды

реакцияны тудыруға арналған [11].

Электрондық құпиялылыққа қатысты алаңдаушылық шын мәнінде негізді болуы мүмкін, көптеген киберқылмыстар қауіпсіздікті бұзудың тікелей нәтижесі болып табылады [12; 13].

Халықаралық стандарттау ұйымы қазіргі уақытта киберқауіпсіздікті киберкеңістіктегі ақпараттың құпиялылығын, тұтастығын және қол жетімділігін сақтау ретінде анықтайды [26], киберкеңістікті технологиялық құрылғылар мен оған қосылған желілер арқылы адамдардың, бағдарламалық жасақтаманың және қызметтердің өзара әрекеттесуінен туындайтын күрделі орта ретінде байланыстыра отырып, ешқандай физикалық тұрғыдан жоқ нысаны [15].

Материалдар мен әдістер

Зерттеу барысында шетелдік дереккөздерге талдау жүргізілді, олардан Еуропа мен Азия елдерінде киберқауіпсіздік саласында оқыту және кәсіптік даярлау бойынша белсенді жұмыс жүргізіліп жатыр деген қорытынды жасауға болады; зерттеудің теориялық-әдіснамалық негіздері айқындалды және ғиберқауіпсіздік бойынша информатика мұғалімдерін даярлаудың ерекшелігі ашылды.

Әдебиетке шолу

Информатика мұғалімдерінің кәсіби құзыреттілігін қалыптастыру көптеген авторлардың ғылыми еңбектерінде қарастырылады. Сонымен, А.И. Блинкин XXI ғасырдағы информатика мұғалімінің кәсіби құзыреттілігін қарастырады және мұғалімдердің үздіксіз өзін-өзі тәрбиелеу және олардың заманауи ақпараттық технологиялар саласындағы құзыреттілігін арттыру қажеттілігі туралы қорытынды жасайды [2].

Цифрлық білім беру жағдайында болашақ информатика мұғалімдерін даярлауды Е.В. Баранова мен И.В. Смирнова қарастырды, олар информатика мұғалімінің кәсіби құзыреттілігін қалыптастыруды қамтамасыз ететін педагогикалық білім бакалаврларын даярлау моделін ұсынды. Өз зерттеулерінде авторлар дайындықтың құрылымы мен мазмұны қоғамның жеке үміттері мен білім беру талаптарына және еңбек нарығының қажеттіліктеріне сәйкес келуі керек деген қорытынды жасайды [1].

Информатика мұғалімдерінің кәсіби құзыреттілігін қалыптастыруда пәнаралық әдістемелік жүйені қолдануды П.В. Никитин ұсынады. Педагогикалық жоғары оқу орындарында оқу барысында кәсіби құзыреттілікті қалыптастыру проблемаларын сипаттай отырып, болашақ информатика мұғалімдерінің кәсіби дайындығын жетілдіру қажеттілігін көрсетеді [14].

Қашықтықтан оқыту форматында ақпараттық қауіпсіздік мәдениетін қалыптастыруға А.В. Наумова мен Е.Г. Топоркованың ғылыми зерттеулері бағытталды. Авторлар қашықтықтан білім беруді, сондай-ақ оқытудың тиімділігіне әсер ететін мұғалімнің қажетті дағдылары мен құзыреттерін қарастырды [5].

Ақпараттық қауіпсіздікті және ақпаратты қорғауды қамтамасыз ету, әлемдік ақпараттық қоғамдастықта жеке тұлғаның қауіпсіздігін қамтамасыз ету проблемасының маңыздылығы туралы идеяны әзірлеуді Е.В. Чернова қарастырады және ақпараттық мәдениеттің негізгі элементтерін қалыптастыру жеке тұлғаның табысты дамуы мен кәсіби өсуі үшін маңызды ақпараттық және жалпы мәдени құзыреттерді дамытуға мүмкіндік береді деген қорытынды жасайды [18].

Болашақ мұғалімдердің киберқауіпсіздікті қамтамасыз ету бойынша кәсіби құзыреттіліктерін қалыптастыру кезінде оқытудың интерактивті әдістерін қолдану мәселесі Т. В. Рихтердің ғылыми жұмысында қарастырылған. Ғалым Киберқауіпсіздіктің құрамдас бөліктерін, киберқауіпсіздікті қамтамасыз ету саласындағы педагогтердің кәсіби

құзыреттілігінің жекелеген элементтерін қалыптастыруға ықпал ететін интерактивті әдістер топтарын бөліп көрсетеді [17].

Киберқауіпсіздік бойынша болашақ информатика мұғалімдерінің кәсіби құзыреттіліктерін қалыптастыру А.А. Нечай мен С.А. Красновтың ғылыми басылымдарында қарастырылған, бұл болашақ информатика мұғалімдерін даярлау бағдарламаларына киберқауіпсіздік негіздерін енгізу қажеттілігін көрсетеді [6; 9].

Нәтижелер

Киберқауіпсіздік көптеген пікірталастардың, қызығушылықтың және назар аударудың саласы екені анық.

Сондай-ақ, «киберқауіпсіздік» ұғымын айтарлықтай жеңілдетуге болады. Киберқауіпсіздікті бірнеше негізгі терминдерге және олардың қарым-қатынастарына жеңілдету икемді құрылымды қамтамасыз етеді. Бұл икемділік деңгейі оқу бағдарламаларына киберқауіпсіздік анықтамаларында, стандарттарында және құрылымдарында мәселелерді шешуге көмектесетін салыстырмалы түрде ашық академиялық құрылымды сақтауға көмектеседі. Киберқауіпсіздікке баса назар аударуды ақпараттық қауіпсіздік пен Ақпарат қауіпсіздігінің жалпы алғышарттарын ұстанатын үш санат бойынша шектеуге болады [16]: бұл «дайындық», «қорғау» және «әрекет» категориялары. Бастапқыда киберқауіпсіздік киберқауіпсіздікке реакцияны білдіретін «реакция» санаттарымен белгіленді. Аксиоманы ескере отырып, бұл орынсыз болып көрінді: «әрекет еткеннен гөрі әрекет ету жақсы». «Реакция» санаты жақсы орындалған әрекет жоспарынан гөрі абайсыз реакцияны тудыруы мүмкін. Осы санаттардың әрқайсысы келесі сұрақтар арқылы жақсы контексттелген болуы мүмкін:

1. Қандай киберқауіптер бар, біз оларға қалай дайындалып, ықтимал шабуылдарды азайта аламыз? (Дайындық).

2. Ақпараттық жүйелерді қалай жобалауға және қауіпсіз ұстауға болады? (Қорғау).

3. Кибершабуыл болған жағдайда не істеу керек және қолда бар қорғаныс құралдарын қалай қолдануға болады? (Әрекет).

Киберқауіпсіздікке дайындық тәуекелдердің түсінікті екенін білдіреді [27]. Бұл қауіп пен оның салдарын терең түсінуді талап етеді. Маңыздысы, олар тек техникалық емес. Дайындықтың көп бөлігі киберкеңістік пен нақты әлем арасындағы байланысты түсіну болып табылады. Негізгі техникалық тақырыптар-ену сынағы, этикалық бұзу және жетілдірілген тұрақты қауіптер [28].

Киберқорғау компьютерлік жүйелерді қорғау бойынша алдын алу шараларын қабылдауды қамтиды және қайтадан техникалық және техникалық емес элементтерді қамтиды. Бұл санат жүйені басқару үшін жақсы жұмыс істейді деп санаймыз. Жүйе әкімшілері жүйелер мен желілерге техникалық қызмет көрсетуге, сондай-ақ қауіпсіздік саясатын жүзеге асыруға жауапты [29]. Басқа тиісті тақырыптар қауіпсіздік контекстінде желілер мен жүйелерді жобалауды қамтиды. Пайдаланушыларды даярлау, аудит, аккредиттеу және оқыту-мұның бәрі профилактикалық қорғау санатына жатады [30].

Әрекет категориясы – бұл кибершабуыл болған жағдайда жасалуы керек нәрсе. Белсенді шабуылдың белгілері қандай, ықтимал әсерді бағалау, атрибуция алу, жауап беру және қызметті қалпына келтіру үшін қандай қадамдар жасау керек? Техникалық тақырыптарға сандық сот сараптамасы (нақты және офлайн) және оқиғаларға жауап беру кіреді. Басқа салаларға мәдени және жаһандық стандарттау, құқықтық мәселелер, қарсы сараптама, компьютерлік криминалистика және оқиғаларға жауап беру теориясы және әртүрлі ұйымдардың әртүрлі әдістемелер мен басымдықтарға ие екенін түсіну кіреді [19].

Киберқауіпсіздік-бұл жаңа тақырып емес, керісінше, біртұтас талдау, түсіну, киберқауіптерден қорғау және оларға жауап беру үшін бар білімді қарау және корреляциялау әдісі.

Оқытуда дәйекті тәсілмен болашақ информатика мұғалімдерін бастапқы оқыту

ақпараттық және киберқауіпсіздік білім беру саласындағы жоғары басымдық мәселесі ретінде, әсіресе мұғалімдерді даярлаудың жалпы жүйесі шеңберінде оқу бағдарламалары ішінде және оларда киберқауіпсіздік саласында кәсіби құзыреттіліктерді қалыптастыру мәселесі ретінде оқытылуы тиіс жерде қажет [31].

Мұғалімге цифрлық қауіпсіздік туралы Білім және оған жету жолдары қажет екеніне күмән жоқ. Мұғалімдер цифрлық қауіпсіздікті оқытуды өз мойнына алады және оқушыларын интернеттегі мінез-құлық ережелеріне бағыттайды деп күтілуде, бірақ мұғалімдер көбінесе этикалық емес мінез-құлықпен байланысты тәуекелдерді түсіну үшін жеткілікті дайындықтан өтпейді. Оқытушы ақпараттық технологияларды қолдану кезінде студенттердің мінез-құлқын жақсартуға, тәуекелдер мен зиян туралы әңгімелер жүргізуге және студенттерге өз іс-әрекеттерімен айтарлықтай әсер етуге көмектесетін модель бола алады.

Осылайша, киберқауіпсіздікті алғашқы оқыту болашақ мұғалімдердің инновациялық процестерге бейімделуі және заманауи ақпараттық технологияларды пайдалану үшін еңбек нарығында бәсекеге түсуі үшін Қоғамның қазіргі қажеттіліктеріне сезімтал болуы керек. Жаңа цифрлық мәдениет мұғалімдерден цифрлық қоғамда пайдалы және сұранысқа ие болуды талап етеді.

Әр түрлі зерттеулер білім беру саласындағы басым мәселелер ретінде қауіпсіздікті арттыру үшін Киберқауіпсіздік бойынша дайындыққа кепілдік беретін білім беру мекемелері үшін орталықтар құру қажеттілігін көрсетеді, әсіресе бұл болашақ мұғалімдерді даярлау бағдарламаларына қатысты.

Халықаралық деңгейде, Еуропа және Азия елдерінде киберқауіпсіздік саласында оқыту және кәсіптік даярлау жолымен қауіпсіздікті арттыру бойынша жұмыстар жүргізілуде.

Мысалы, Тайваньда «Таис» бағдарламасы білікті мұғалімдерді даярлаудың төрт аспектісін анықтады:

- байланыс қауіпсіздігі және қорғау;
- ақпараттың жарамдылығы;
- Интернеттегі қауіпсіздік;
- технологиялық құрылғыларды өз бетінше пайдалану.

ЕО елдерінде Британдық Білім беру коммуникациялары және технологиялар агенттігі «ВЕСТА» сияқты ұйымдар, Скандинавия елдері мен Чехиядағы әртүрлі зерттеулер мұғалімдерді даярлаудың маңыздылығын атап көрсетеді және алдыңғы тәжірибе, білім, тәжірибе, пікірлер мен қабылдау мұғалімдердің киберқауіпсіздік мәселелерін қалай үйрету, шешу және шешу керектігін анықтайды деген қорытындыға келеді [20]. деңгейде

Жаһандық «ЮНИСЕФ» (Біріккен Ұлттар Ұйымының Халықаралық Балалар қоры) білім беру мекемелері үшін іс – қимылдар мен білім беру шараларын шоғырландырудың маңыздылығын және олардан ата-аналар мен мұғалімдердің бірлескен жауапкершілігін, сондай-ақ қауіптерді болдырмауға және цифрлық әлемнің қауіптерінен қорғауға көмектесетін білім беру және алдын алу бағдарламаларына білім беру ресурстарын бөлу қажеттілігін ұсынады.

Талқылаулар мен қорытындылар

Білім беру қажеттіліктерін анықтау мақсатында Киберқауіпсіздік бағыты бойынша болашақ мұғалімдерді даярлауға байланысты шет елдердің озық тәжірибесіне және тақырыпқа сәйкес ғылыми жарияланымдарға зерттеулер жүргізе отырып, болашақ маманды даярлау үшін шешуші маңызы бар бірқатар тақырыптар ұсынылды:

- онлайн байланыс және мінез-құлық ережелері (желілік этикет);
- интернеттегі тәуекелдердің алдын алу және физикалық және психикалық денсаулыққа қамқорлық жасау шаралары мен құралдары;

- цифрлық қауіпсіздікке байланысты тұжырымдамалар (бедел, сәйкестілік, цифрлық алшақтық және саусақ ізі);
- білім беру саласындағы дербес деректерді қорғау;
- құрылғыларды қауіпсіз қорғау және парольдер жасау.

Киберқауіпсіздік туралы арнайы зерттеулер аз болғанымен, тақырыптың өзектілігі оның ақпараттық технологиялармен байланысты жетекші компаниялар мен ұйымдардың күн тәртібіндегі тұрақты талқылауымен расталады. Нәтижесінде, бұл киберқауіпсіздікті оқыту, сондай-ақ осы тақырыпты ілгерілету және оны білім берудің әртүрлі кезеңдеріндегі қолданыстағы оқу жоспарлары мен бағдарламаларына енгізу бойынша тереңдетілген зерттеулердің қажеттілігін көрсетеді.

References

[1] Baranova, E.V., Simonova, I.V. Razvitie professional'nyh kompetencij bakalavrov po napravleniyu pedagogicheskogo obrazovaniya v oblasti informatiki v usloviyah cifrovogo obrazovaniya Izvestiya Rossijskogo gosudarstvennogo pedagogicheskogo universiteta im. A.I. Gercena. 2018. 190. 116– 124. (In Russian).
[2] Blikin, A.I. Professional'nye kompetencii uchitelya informatiki XXI veka V sbornike: Innovacionnye tekhnologii XXI veka. materialy Mezhdunarodnoj nauchno-prakticheskoj konferencii. Kazanskij gosudarstvennyj tekhnicheskij universitet im. A.N. Tupoleva. 2015. 81–82. (In Russian).
[3] Borisov, A.A., Krasnov, S.A., Nechaj, A.A. Tekhnologiya blokchejn i problemy eyo primeneniya v razlichnyh informacionnyh sistemah. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. 2018. 2. 63– 67. (In Russian).
[4] Kalinichenko, S.V., Kotikov, P.E., Nechaj, A.A. Reshenie replikacionnyh problem v bazah dannyh dlya povysheniya ustojchivosti programmnogo obespecheniya avtomatizirovannyh system. Bulletin of the Russian New University. Series: Complex Systems: Models, analysis and management. 2017. 4. 18–21. (In Russian).
[5] Naumova, A.V., Toporkova, E.G. Formirovanie kul'tury informacionnoj bezopasnosti v formate distancionnogo obucheniya. V sbornike: Informacionnye problemy i drajvery social'no-ekonomicheskogo razvitiya obshchestva v usloviyah globalizacii. Sbornik nauchnyh statej Mezhdunarodnoj nauchno-prakticheskoj konferencii. Stavropol'skij gosudarstvennyj Agrarnyj universitet. 2020. 479–481. (In Russian).
[6] Nechaj, A.A. Formirovanie professional'noj kompetencii v oblasti kiberbezopasnosti u budushchih uchitelej informatiki. Vestnik Leningradskogo gosudarstvennogo universiteta im. A.S. Pushkina. 2020. 4. 114–124. (In Russian).
[7] Nechaj, A.A. Gejmifikaciya kak sposob organizacii obucheniya kiberbezopasnosti. V knige: Fundamental'nye problemy obucheniya matematike, informatike i informatizacii obrazovaniya. Sbornik tezisov dokladov mezhdunarodnoj nauchnoj konferencii, posvyashchennoj 180letiyu pedagogicheskogo obrazovaniya v g. El'ce. 2020. 93–94. (In Russian).
[8] Nechaj, A.A. Kiberbezopasnost' i informacionnaya bezopasnost', sushchnost', soderzhanie i otlichie ponyatij. V sbornike: XXIV Carskosel'skie chteniya. 75letie Pobedy v Velikoj Otechestvennoj vojne. Materialy mezhdunarodnoj nauchnoj konferencii. Pod obshchej redakciej S.G. Eremeeva. 2020. 229–232. (In Russian).
[9] Nechaj, A.A., Krasnov, S.A. 2020. Formirovanie kompetencii uchitelya informatiki v oblasti kiberbezopasnosti. Azimut nauchnyh issledovanij: pedagogika i psihologiya. T.9. Vol. 4(3). pp. 188–190. (In Russian).
[10] Nechaj, A.A. Ispol'zovanie innovacionnyh metodov i sovremennyh tekhnologij dlya povysheniya kvalifikacii v oblasti kiberbezopasnosti. Azimut nauchnyh issledovanij: pedagogika i psihologiya. 2020. 3(32). 193–196. (In Russian).
[11] Nechaj, A.A. Formirovanie bezopasnoj informacionnoj sredy. Aktual'nye problemy sovremennosti: nauka i obshchestvo. 2019. 4(25). 43–44. (In Russian).
[12] Nechaj, A.A., Krasnov, S.A., Svinarchuk, A.A. Analiticheskaya model' obespecheniya informacionnoj bezopasnosti obrazovatel'nyh organizacij sistemy obshchego i srednego obrazovaniya. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. 2020. 4. 77–84. (In Russian).

[13] Nechaj, A.A., Kotikov, P.E. Aktual'nye problemy zashchity informacii v sovremennyh avtomaticheskih telefonnyh stanciyah. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. 2015. 2. 65–69. (In Russian).
[14] Nikitin, P.V. Mezhdisciplinarnaya metodicheskaya sistema formirovaniya professional'noj kompetentnosti u budushchih uchitelej informatiki. Vestnik CHuvashskogo gosudarstvennogo pedagogicheskogo universiteta im. I.YA. YAkovleva. 2015. 3-2(67). 135–140. (In Russian).
[15] Novikov, A.N., Nechaj, A.A., Malahov, A.V. O podhode k obosnovaniyu racional'noj nomenklatury etalonnoj bazy izmeritel'nyh kompleksov na osnove nechetkih modelej. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. 2017. 1. 72–79. (In Russian).
[16] Novikov, A.N., Nechaj, A.A., Malahov, A.V. Matematicheskaya model' obosnovaniya variantov rekonfiguracii raspredelennoj avtomatizirovannoj kontrol'no-izmeritel'noj sistemy Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. 2016. 1-2. 56–59. (In Russian).
[17] Rihter, T.V. Ispol'zovanie interaktivnyh metodov obucheniya pri formirovanii professional'nyh kompetencij pedagogov po obespecheniyu kiberbezopasnosti podrastayushchego pokoleniya. V knige: Aktivnye i interaktivnye metody obucheniya v estestvenno-matematicheskom obrazovanii. Kollektivnaya monografiya. Solikamskij gosudarstvennyj pedagogicheskij institut (filial) FGBOU VO «Permskij gosudarstvennyj nacional'nyj issledovatel'skij universitet». Solikamsk. 2018. 13–21. (In Russian).
[18] CHernova, E.V. Informacionnaya bezopasnost' cheloveka. Uchebnoe posobie / Moskva. Vysshee obrazovanie (2-e izd., ispr. i dop). 2020. 76. 24. (In Russian).
[19] SHirobokov, V.V., Nechaj, A.A. Algoritm planirovaniya energosberegayushchej parallel'noj obrabotki informacii s uchetom informacionnoj vazhnosti i vremeni postupleniya zadach. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie 2017. 1. 88–93. (In Russian).
[20] Esaulov, K.A., YAhvarov, E.K., Nechaj, A.A., Berezin, A.S. Metodika integracii sistemy upravleniya kiberriskami v predprinimatel'skih strukturah. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie. Vestnik Rossijskogo novogo universiteta. Seriya: Slozhnye sistemy: modeli, analiz i upravlenie 2020. 2. 80–86. (In Russian).
[21] Bentle M., Stephenson A., Toscas P., Zhu Z. A multivariate model to quantify and mitigate cybersecurity risk. 2020. 8. 1-21.
[22] Jeyaraj A., Zadeh A., Sethi V. Cybersecurity threats and organisational response: textual analysis and panel regression. Journal of Business Analytics. 2020.
[23] Kavallieratos G., Katsikas S., Gkioulos V. Cybersecurity and safety co-engineering of cyberphysical systems – a comprehensive survey. Future Internet. 2020. 12. 65.
[24] Li, Y., Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. International Journal of Production Research. 2021. 4. 1216–1238.
[25] Panigrahi, R., Borah, S. A statistical analysis of lazy classifiers using canadian institute of cybersecurity datasets. Lecture Notes on Data Engineering and Communications Technologies. 2020. 37. 215–222.
[26] Pohasii, S.S., Milevskyi, S.V., Milevskyi, S. Cybersecurity issues in the internet of things. Black Sea Scientific Journal of Academic Research. 2020. 48. 135–137.
[27] Toapanta, S.M.T., Jaramillo, J.M.E., Gallegos, L.E.M. Cybersecurity analysis to determine the impact on the social area in latin america and the Caribbean. ACM International Conference Proceeding Series. 2. Cep. "ICETM 2019. 73–78.
[28] Toapanta, S.M.T., Armijos, M.A.A., Gallegos, L.E.M. Analysis of cybersecurity models suitable to apply in an electoral process in ecuador ACM International Conference Proceeding Series. 2. Cep. "ICETM 2019. 84–90.
[29] Fernández-Caramés, T.M., Fraga-Lamas, P. Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. Sensors. 2020. 20. 30–48.
[30] Xu S. Cybersecurity dynamics: a foundation for the science of cybersecurity Advances in Information Security. 2019. 74. 1–31.
[31] Nechay, A. A. Orientirovannost' podgotovki budushchikh uchitelej informatiki na formirovanie professional'nykh kompetencij po informacionnoj bezopasnosti. Vestnik Leningradskogo gosudarstvennogo universiteta imeni A.S. Pushkina – Pushkin Leningrad State University Journal. 2021. 2.

МЕТОДИЧЕСКИЕ ОСНОВЫ ПОДГОТОВКИ БУДУЩИХ УЧИТЕЛЕЙ ИНФОРМАТИКИ НА ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ПО

КИБЕРБЕЗОПАСНОСТИ

Мекебаев Н.О[1]., Назкенова Б.Б[1]., Чайко Е.В[2].
[1]Казахский национальный университет им. аль-Фараби, г.Алматы, Казахстан
[2]Рижский технический университет, Латвия, Рига
nurbapa@mail.ru, nazkenova_bayan@mail.ru, jelena.caiko@gmail.com
ORCID:0000-0002-9117-4369
ORCID: 0000-0002-6671-7835
ORCID: 0000-0002-1207-1418

Аннотация. Информационная безопасность является глобальной проблемой из-за растущей зависимости общества от глобальной сети Интернет, а киберугрозы – один из самых серьезных вызовов для экономики и национальной безопасности. Информационная безопасность стала главным национальным приоритетом. Все организации, включая образовательные учреждения, работающие с применением цифровых компьютерных технологий, нуждаются в специалистах, обладающих компетенциями и навыками, которые включают поведенческие, управленческие и технические знания для борьбы с кибератаками в динамичной среде киберугроз. В связи с этим растет спрос не только на квалифицированных специалистов, но и на учителей, обладающих компетенциями по информационной безопасности, которые способны учить основам кибербезопасности со школьной скамьи.

Существующие противоречия между повсеместным применением цифровых технологий, уязвимых к кибератакам, и недостаточностью использования образовательного процесса для обучения информационной безопасности, а также между увеличением спроса на подготовку учителей информатики по информационной безопасности и недостаточной готовностью профессорско-педагогического состава вуза к подготовке соответствующих специалистов позволяют сформулировать актуальную проблему научного исследования, которая заключается в необходимости системного обеспечения подготовки будущих учителей информатики и формирования у них профессиональных компетенций по информационной безопасности в современных условиях развития информационного общества. Новизна исследования состоит в разработке подхода к обучению будущих учителей информатики основам кибербезопасности и формированию у них компетенций по информационной безопасности в условиях цифровизации образования.

Ключевые слова: учитель информатики, информационная безопасность, кибербезопасность, профессиональная подготовка, компетенция.

METHODOLOGICAL FOUNDATIONS OF THE TRAINING OF FUTURE COMPUTER SCIENCE TEACHERS FOR THE FORMATION OF PROFESSIONAL COMPETENCIES IN CYBERSECURITY

Mekebayev N[1], Nazkenova B[1]., Chaico E.[2]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Riga Technical University, Latvia, Riga
nurbapa@mail.ru, nazkenova_bayan@mail.ru, jelena.caiko@gmail.com
ORCID:0000-0002-9117-4369
ORCID: 0000-0002-6671-7835
ORCID: 0000-0002-1207-1418

Abstract. Information security is a global problem due to the growing dependence of society on the global Internet, and cyber threats are one of the most serious challenges to the economy and national security. Information security has become a top national priority. All organizations, including educational institutions, working with the use of digital computer technologies, need specialists with competencies and skills that include behavioral, managerial and technical knowledge to combat cyber attacks in a dynamic environment of cyber threats. In this regard, there is a growing demand not only for qualified specialists, but also for teachers with information security competencies who are able to teach the basics of cybersecurity from the school bench.

The existing contradictions between the widespread use of digital technologies that are vulnerable to cyber attacks, and the lack of use of the educational process for teaching information security, as well as between the increasing demand for training computer science teachers in information security and the lack of readiness of the university's teaching staff to train relevant specialists, allow us to formulate an urgent problem of scientific research. The problem lies in the need for systematic training of future teachers of computer science and the formation of their professional competencies in information security in the modern conditions of the development

of the information society. The novelty of the research is the development of an approach to teaching future computer science teachers the basics of cybersecurity and the formation of their competencies in information security in the context of digitalization of education.

Keywords: computer science teacher, information security, cybersecurity, professional training, competence.

Авторлар жайында мәлімет:

Қаз: Мекебаев Нұрбапа Отанұлы – Әл-Фараби атындағы Қазақ ұлттық университетінің PhD, nurbapa@mail.ru

Рус: Мекебаев Нурбапа Отанович – PhD, Казахский национальный университет им. аль-Фараби, nurbapa@mail.ru

Англ: Nurbapa Otanovich Mekebayev – PhD, Al-Farabi Kazakh National University, nurbapa@mail.ru

Қаз:Назкенова Баян- Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, nazkenova_bayan@mail.ru

Рус: Назкенова Баян- докторант Казахского национального университета имени Аль-Фараби, nazkenova_bayan@mail.ru

Англ: Naskenova Bayan is a doctoral student at Al-Farabi Kazakh National University, nazkenova_bayan@mail.ru

Қаз: Чайко Елена Валерьевна - PhD, Рига техникалық университетінің профессоры, jelena.caiko@gmail.com

Рус: Чайко Елена Валерьевна – PhD, профессор Рижского технического университета, jelena.caiko@gmail.com

Англ: Elena V. Chaiko – PhD, Professor of Riga Technical University, jelena.caiko@gmail.com