Қорытынды

ЖОО зияткерлік капиталды бағалаудың бірден бір әдісі ретінде ТКЖ бірнеше алдыңғы қатарлы университеттерде енгізіліп, тәжірибеден өткізілген. Атап айтсақ: Лос-Анджелестегі Калифорния университеті, Индиана университеті, Эдинбург университеті, Карлтон университеті және т.б. Теңгерімді көрсеткіштер жүйесінің артықшылығы мынада, менеджерлерге негізгі стратегиялық мәселелерге назар аударуды ұсына отырып, ол қызмет көрсеткіштерінің жалпы санын азайтуға мүмкіндік береді, сонымен қатар ұйымды басқару ерекшеліктерін ескереді.

Теңгерімді көрсеткіштер жүйесі университеттің көзқарасы, миссиясы, стратегиясы мен операциялық қызметін мақсаттар мен міндеттерді көрсетумен, сондай-ақ қызмет нәтижелерін бағалаумен байланыстыратын маңызды құрал бола алады. ТКЖ университеттерге енгізудің негізгі себептері:

- маңызды басқару құралы ретінде қарастырылады;
- академиялық бағдарлама мен жоспарлау процестерін бағалауға мүмкіндік береді;
- бұл тек өнімділікті бақылау емес, басқарудың маңыздылығын арттыру құралы.

Пайдаланылған әдебиеттер тізімі:

1. Sutherland, T. (2000). Designing and implementing an academic scorecard. Accounting Education News, 11-13.

2. Cullen, J., Joyce, J., Hassall, T., & Broadbent, M. (2003). Quality in higher education: From monitoring to management. Quality Assurance in Education, 11(1), 5-14.

3. Sutherland, T. (2000). Designing and implementing an academic scorecard. Accounting Education News, 11-13.

4. Chang, O.H., Chow, C.W. (1999). "The Balanced Scorecard: A Potential Tool for Supporting Change and Continuous Improvement in Accounting Education", Issues in Accounting Education, Vol. 14, No. 3, pp. 395-412.

5. Edvinsson L. Managing Intellectual Capital. QFINANCE. P. 1-4. URL:http://www.qfinance.com.

6. Sveiby, Karl-Erik (2001). "A Knowledge-based Theory of the Firm To guide Strategy Formulation", Journal of Intellectual Capital, Vol. 2, No. 4.

7. Kaplan, Robert S. and Norton, David P. (1992). "The Balanced Scorecard", Harvard Business Review,Jan-Feb. pp.71-79.

8. Kaplan, Robert S. and Norton, David P. (1993). "Putting the Balanced Scorecard to Work", Harvard Business Review, pp.134-147.

9. Kaplan, Robert S. and Norton, David P., (1996). "Linking the Balanced Scorecard to Strategy", California Management Review, Vol.39 No.1, , pp.53-79.

10. Holmen, J., (2005). "Intellectual Capital Reporting", Management Accounting Quarterly, 6(4), - pp. 1-9.

ҒТАМР 11.01.29 https://doi.org/10.51889/2020-4.1728-8940.26

*А.У. Нусипова**

Абай атындағы ҚазҰПУ PhD докторанты,
Алматы қ., Қазақстан

КАРАНТИН АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ҚАЛАЙ ӘСЕР ЕТТІ: САЯСАТТАНУЛЫҚ ТАЛДАУ

Аңдатпа

Өткен жылдың аяғынан бастап жаңа COVID-19 инфекциясы адам өмірінің әртүрлі салаларына, соның ішінде заманауи технологиялық құрылымға бұрын-соңды болмаған әсерін тигізді. Жаһандық жағымсыз факторлардың арасында денсаулыққа қатысты қиындықтар да, киберқауіпсіздік мәселелері де атап өтілді.

COVID-19 жаңа пандемиясы пайда болысымен әлем қашықтан қол жетімділіктің қауіпсіздігі проблемаларын объективті және субъективті себептермен анықтй бастады. Бір жағынан, Интернетке үйден кіру нүктесі қауіпсіздік тұрғысынан қиын емес, екінші жағынан, карантинге өту күтпеген

жағдай болды. Қазіргі уақытта ақпараттық қауіпсіздік саласында көптеген жергілікті шешімдер және қауіпсіз қашықтықтан қол жетімділікті ұйымдастыру бойынша халықаралық ұсыныстар бар. Бұл мақалада осы факторлардың өзара байланысы қарастырылады.

Түйін сөздер: COVID-19, ақпараттық қауіпсіздік, ғаламтор, әлеуметтік желілер, ресурстар, ақпараттық технологиялар, карантин.

A.U. Nussipova[*]

PhD doctoral student of Abai KazNPU,
Almaty, Kazakhstan

HOW QUARANTINE AFFECTED INFORMATION SECURITY: A POLITICAL ANALYSIS

Abstract

Since the end of last year, the new COVID-19 infection has had an unprecedented impact on various areas of human life, including the modern technological structure. Among the global negative factors, both health problems and cybersecurity challenges were noted.

Security problems with remote access to the novel coronavirus COVID-19 during a pandemic are identified for objective and subjective reasons. On the one hand, accessing the Internet from home is not difficult from a security point of view, on the other hand, the transition to quarantine was unexpected. Currently, there are many local solutions in the field of information security and international recommendations for organizing secure remote access. The relationship of these factors we will consider in this article.

Key words: COVID-19, information security, Internet, social networks, resources, information technology, quarantine.

А.У. Нусипова[*]

PhD докторант КазНПУ им. Абая,
Алматы, Казахстан

КАК КАРАНТИН ПОВЛИЯЛ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ: ПОЛИТОЛОГИЧЕСКИЙ АНАЛИЗ

Аннотация

С конца прошлого года новая инфекция COVID-19 оказала беспрецедентное влияние на различные сферы человеческой жизни, включая современную технологическую структуру. Среди глобальных негативных факторов были отмечены как трудности здравоохранения, так и вызовы кибербезопасности.

Проблемы с безопасностью удаленного доступа к новому коронавирусу COVID-19 во время пандемии выявляются по объективным и субъективным причинам. С одной стороны, выход в Интернет из дома несложный с точки зрения безопасности, с другой - переход на карантин оказался неожиданным. В настоящее время существует множество локальных решений в области информационной безопасности и международных рекомендаций по организации безопасного удаленного доступа. Взаимосвязь указанных факторов рассматриваются в данной статье.

Ключевые слова: COVID-19, информационная безопасность, Интернет, социальные сети, ресурсы, информационные технологии, карантин.

Кіріспе. Қазіргі қоғамды ақпараттық қоғам деп те атайды. Компьютерлік технологиялар мен коммуникацияның кең дамуы ақпарат жинауға, сақтауға, өңдеуге және ақпаратты беруді өте тиімді және бұрын болмаған көлемде жедел ұсына бастады. Жаңа ақпараттық технологиялардың арқасында адамның өндірістік және өндірістік емес қызметі, оның күнделікті қарым-қатынас саласы әлемдік өркениет қалыптастырған тәжірибе, білім және рухани құндылықтарды тарту есебінен шексіз

кеңейеді, ал экономиканың өзі күннен-күнге материалдық игіліктердің өндірісі ретінде сипатталып, барған сайын ақпараттық өнімдер мен қызметтерді тарату құралы ретінде көрсетілуде.

Ақпараттандырудың қазіргі кезеңі дербес компьютерлік технологияларды, телекоммуникациялық жүйелерді қолданумен, компьютерлік желілерді құрумен тікелей байланысты. Осыған орай ақпараттық индустрияда тиімді шешімдерді әзірлеу және қолдану қажеттілігі артып келеді, бұл жаңа білім алу үшін аппараттық және бағдарламалық жасақтамалар жасаумен және ақпараттық технологиялар шығарумен айналысады. Ақпараттық индустрияның дамуының белгілі бір кезеңінде жұмыскерлердің көп бөлігі ақпаратты өндірумен, сақтаумен, өңдеумен және сатумен айналысатын ақпараттық қоғам туады, яғни бұл қоғам интеллектті дамытуға және білім алуға бағытталған шығармашылық жұмыстар жүргізілуде. Ұлттық шекаралар бойынша бөлінбеген адамдардың бірыңғай ақпараттық қоғамдастығы құрылуда. Ал ақпараттық қоғамның қалыптасуы соңғы ақпараттық, телекоммуникациялық және байланыс технологияларына негізделген. Бұл жаһандық ақпараттық желілердің жылдам таралуына әкеліп соқтырған жаңа технологиялар, халықаралық ақпарат алмасудың принципиалды жаңа мүмкіндіктерін ашты. Ақпараттық қоғамның қалыптасуы тұжырымдамалық және іс жүзінде әлемдік ақпараттық кеңістіктің қалыптасуын білдіреді, сонымен бірге қазіргі карантиндік жағдайға байланысты өте өзекті мәселе болуда.

Ақпараттық сфераның қарқынды дамуы бүкіл әлемдегі қоғам өміріне айтарлықтай әсер етеді, оны бір ғаламдық ақпараттық кеңістікте немесе инфосферада болатын ақпараттық қоғамға біріктіреді. Бұл дегеніміз, қазіргі уақытта ақпараттың шекаралары аз, бұл оң және теріс жағынан оған көбірек адамдар әсер ете алады дегенді білдіреді. Сондықтан ақпараттық ресурстар мен процестер ТМД-да да, әлемнің басқа елдерінде де көптеген әлеуметтік апаттардың түбінде болуы мүмкін екенін ескерген жөн.

Нәтижелерді талдау. Ақпараттық-коммуникациялық технологиялардың, әсіресе компьютерлік технологиялардың дамуы және оларды өмірдің барлық саласында, соның ішінде үкімет пен әскери салада тарату қарама-қайшылықтың немесе қарама-қайшылықтың түбегейлі жаңа түрінің - ақпараттың жақында пайда болуына әкелді. Әрине, ақпараттық соғыстар ұзақ уақыттан бері белгілі және қолданылып келеді деп айтуға болады, бірақ олар насихаттау, бұқаралық ақпарат құралдарын пайдалану, қоғамдық пікірді қолдан жасау, қауесет, алдау, жалған ақпарат және т.б. сияқты құралдарды (және шектеулі) пайдаланды. Технологиялық прогресс ақпараттық соғыстың шын мәнінде жаңа мәнге ие болуына әкелді. Жақында «ақпараттық соғыстар» немесе олардың кибер-аспектілері ақпараттық инфрақұрылым элементтерін рұқсатсыз пайдаланудың, бүлінудің немесе жоюдың және / немесе олардың тұтастығын бұзудың алдын-алу үшін әскери және стратегиялық мақсаттарда көп мөлшерде қолданыла бастады (қорғаныс тұрғысынан) немесе ақпарат саласында артықшылыққа қол жеткізу үшін жаудың ақпараттық инфрақұрылымының элементтерін жою, жолын кесу (яғни шабуылдау). Дегенмен, қару-жарақтың мақсаттары әр түрлі болуы мүмкін және олар тек әскери нысандар болады, және мұндай әрекеттер тек соғыс уақытында ғана жасалады деп айтуға болады - бұл орынсыз және тіпті қауіпті аңғалдықты білдіреді. [1].

Биылғы жылғы бүкіл әлемді дүр сілкіндіріп отырған жаңа коронавирус инфекциясы, пандемия COVID-19 адам өмірінің әртүрлі салаларына, оның ішінде қазіргі технологиялық құрылымына бұрын-соңды болмаған әсерін тигізді. Қазіргі уақытта әлем бойынша жүздеген миллион адам интернет көмегімен үйден жұмыс істеуге мәжбүр. Ғаламтор желісін уақытты жағымды өткізу құралы деп ғана білетіндердің өзі бүгін оны қызметінде туындаған мәселелерді шешу үшін белсенді қолдана бастаған. Виртуалды кездесулерді жүзеге асыру мен отбасының тұрмыстық қажеттілігін қамтамасыз етуде керек-жарақты сатып алу да тек интернет арқылы қолжетімді. Қызметті қашықтан атқару барысында компьютер желісі мен интернет-сервистердің маңызы еселенген кезде, кибер қылмыскерлердің де белсенділігін арттырып отыр. Олар өзекті жаңалықтарды, төтенше жағдай туралы хабарларды жіберіп, желі қоданушыларын сілтемелер арқылы зиянды сайттарға өтуге итермелеуге тырысады. Вирустық бағдарламар бар хаттарды жолдайды, нәтижесінде өз көздеген мақсаттарына жетуге жол табады [2].

Кибер қылмыскерлер әдетте қаржы саласында жұмыс жасайтын мекемелердің қас жауы болады, көбінесе солардың ақпараттық қорына қол жеткізуді көздейді. Көптеген компания мамандары осы шабуылдарды көріп қана қоймай, оның салдары қандай болатынын сараптап, қылмыстың алдын алуды жетік меңгерген. Бұл жұмыстар үнемі бақылауды, талдауды және болжауды талап етеді. Дегенмен, әлеуметтік қашықтықты қажет етіп тұрған дағдарысқа дайын емес компаниялар да

жеткілікті. Арасында өз жұмысын уақытша доғарғандар бар. Алайда, киберқауіпсіздік тұрғысынан қауіпті жағдайда қызметін жалғастырғандар да жоқ емес. Европолдың мәліметінше, коронавирустың өршуі кезінде DDos-шабуылдар саны артқан. Қылмыскерлер аталмыш шабуылдарын жүзеге асырмауы немесе тоқтатуы үшін ақша талап етеді. Алып компаниялар жиі осындай әрекеттердің құрбаны болады.

DdoS-шабуыл онлайн-сервистердің жұмысын бұзуға бағытталған. Заңсыз трафик ағымының арқасында компьютерлер, Интернет және сұранысты жіберетін басқа да құрылғылар көмегімен бір уақытта көптеген сұраныстар жіберіледі. Бұл, сайып келгенде, қызметті шамадан тыс жүктейді. Бұл ретте нақты тұтынушылар немесе пайдаланушылар кері байланыс ала алмайды. DDoS шабуылдары әдетте ресурс қорын азайтады.

Бұқараның коронавирус төңірегіндегі үрейі киберқылмыскерлер үшін фишинг шабуылдарды жасауға жағдай жасап отыр. Салдарынан еш қауіп тудырмайтындай көрінген хат арқылы зиынды бағдарламалар таратылуда [3].

Біз әлеуметтік шабуылдарды қылмыстық (тұрмыстық) деңгей мен кибер операциялардың (мемлекеттік немесе өндірістік сипаттағы) деңгейіне қарай ажыратуға болады. Үй шаруашылығында, өздеріңіз білетіндей, кибершабуылдар шартты түрде екі сыныпқа бөлінеді:

- тұлғаның жеке басын және басқа да жеке ақпаратты заңсыз алу мақсаты болып табылатын фишингтік шабуылдар;
- ақшаны заңсыз алуға немесе банктік шоттарға қол жеткізуге бағытталған қаржылық алаяқтық.

Кибероперациялар мен АПТ шабуылдарының деңгейіне, зиянды пошта таратудың дәстүрлі тізімдері, саяси қате ақпарат пен троллинг, сонымен қатар шабуылдың салыстырмалы түрде жаңа түрі, адамдарды іздеуге бағытталған қосымшалардың орнатылуы әдебиеттегі коронавирус тақырыбымен байланысты.

Фишингтік шабуылдардың бірнеше түрлері бар, атап айтқанда: Интернет-ресурстарды (пошта, веб-парақтар) дәстүрлі түрде пайдалану, мәтіндік / SMS хабарламалар (белсенді әрекетті бастау, мысалы, жалған дауыс беру арқылы алдау арқылы) және дауыстық хабарламалар (атап айтқанда, VoIP хаттамасы).

COVID-19 коронавирустық инфекциямен байланысты әйгілі әлеуметтік инженерлік шабуылдардың мысалдары бойынша:

1. Әдетте фишинг немесе ақша бопсалау мақсатында зиянды қосымшасы бар немесе зиянды бағдарлама / веб-сайтқа сілтеме бар электрондық поштаны жіберу. Мұндай хаттардың көздері әдетте заңды болып жасырылады, мысалы, денсаулық сақтау ұйымы ретінде (әдетте БҰҰ Дүниежүзілік денсаулық сақтау ұйымы), компанияның директоры, АТ қолдау қызметі (немесе керісінше, егер хат АТ-қолдау қызметіне жіберілсе, карантин кезеңінде дереккөз заңды қолданушы ретінде маскировкаға түседі) сақтандыру компаниясы (мысалы, хабарлама мәтіні алушының эпидемия кезінде медициналық сақтандырудың аяқталғанын көрсетеді), қайырымдылық коммерциялық емес компания, қаржы немесе сауда компаниясы (пандемия кезіндегі өте жақсы ұсыныспен), оқу орталығы, провайдер (әдетте Қытайдан келетін электроника), компания салығы, туристік немесе авиакомпания, еңбек биржасы және т.б. TrenMicro зерттеуіне сәйкес, әлеуметтік шабуылдардың 65% -дан көбі – спам хаттар [4].

2. Зиянды қосымшаларды орнатуға арналған ұсыныстар, мысалы, коронавирустың таралу картасы (геологиялық орналасу нүктесінің жанында жалған вирустық тасымалдаушыларды көрсететін) - Коронавирус немесе Ginp картасы.

3. Денсаулық сақтау ұйымдары, қайырымдылық ұйымдары, сақтандыру компаниялары, вирусқа қарсы препараттарды ақысыз тарататын ұйымдар сияқты жалған веб-порталдарға кіру (сіз «жеткізу үшін» төлеуіңіз керек деген ақпараттар болады) және басқалар. Қауіпсіздік саласындағы сарапшылар жалған фишингтік веб-сайттардың пайда болуының қайталану толқынын тіркеді, олардың аты енді *covid* емес, қашықтан қол жеткізудің туынды фразалары - *teams* немесе *zoom* (бейнеконференция қосымшалары).

4. Жасанды жаңалықтар, (Денсаулық сақтау министрлігі немесе әкімдіктердің) жедел хабарлары, карантиндік QR кодын жасау немесе қорқыныш, стресс және денсаулыққа зиян паразит материалдар, мысалы, жаһандық қастандық теориясына қатысты (биологиялық соғыс, оқудың тасталуы, климаттың өзгеруімен және әртүрлі обсурантизм көріністерімен күресу), сайып келгенде, зиянды ресурстарға сілтеме жасайды.

Британдық ғалымдардың зерттеуі бойынша, компьютерлік шабуылдардың 98% -ында әлеуметтік инженерия әдістері қолданылады [5].

Мәселен, коронавирустан қорғану туралы ақпарат, Дүниежүзілік денсаулық сақтау ұйымының кезекті мәлімдемесі немесе бетперде мен өзге де дезинфекциялық құралдардың сатылуы жайында хаттарды ашып оқудың өзі бүгін қауіп төндіреді [6]. Себебі, осы арқылы сізге зиянды бағдарламар мен вирус жіберілуі мүмкін. Нәтижесінде, алаяқтар Windows жүйесіндегі құпия сөз, қолданушылардың есім-сойлары мен банктегі реквизиттер жайындағы мәліметті қолды қылады.

Осы жағдайға байланысты Дүниежүзілік денсаулық сақтау ұйымы ескерту жариялаған. Өзін аталмыш ұйым қызметкері деп таныстырған адаммен сөйлесу кезінде асқан қырағылық пен сақтық танытуды өтінген. Себебі бұл қазіргі ахуалды өз мүдделері үшін пайдаланып отырған киберқылмыскер болуы әбден мүмкін екенін ескертеді. Мамандардың айтуынша, айына орта есеппен 1,4 миллион осындай жалған сайттар жасалады екен [7].

Қазіргі жағдайға байланысты мамандарының айтуынша, қашықтан жұмыс жасау барысында бірнеше қағиданы есте сақтау абзал. Ең негізгісі поштамен сауатты жұмыс жасай білу қажет. Бейтаныс адресаттан келген хаттағы сілтемеге басудан, лицензиясы жоқ бағдарламаларды жүктеуден және орнатудан бас тартқан дұрыс, яғни «цифрлық тазалықты» сақтау маңызды.

Халықаралық электробайланыс одағының (ХЭО) есебіне сәйкес, Қазақстан 2018/2019 жж ғаламдық киберқауіпсіздік индексінде 40 орынға ие болған. Primeminister.kz ресми ақпарат ресурсында еліміздің 2017/2018 жж аталмыш рейтингте 82-орында болғаны жазылған [8].

Қорытынды. COVID-19 коронавирусының жаңа инфекциясы басталған кезде бүкіл АТ әлемі ақпараттық қауіпсіздік саласында ерекше міндетке тап болды, және пандемия кезінде компьютерлік желілерде қауіпсіз жұмыс істеу тәжірибесін ескере отырып ұйымдастыру және техникалық тұрғыдан алғанда баға жетпес екеніне көз жеткізді.

Осы дағдарыс кезеңінде қоғамдық ақпараттық жүйелерге қол жетімділіктің бұзылуы (ел экономикасын цифрландыруды ескере отырып) жоғары технологиялық бағдарламалық қамтамасыз етуді және ақпаратты қорғаудың болашақ құралдарын одан әрі жетілдіру қажеттілігін көрсетті.

COVID-19 коронавирусының таралуынан кейін әлем бұрынғыдай болмайды деп философиялық түрде болжауға болады. «Жаңа шындық» идеясы жаппай тестілеуді бастағаны анық (қашықтықтан жұмыс және оқыту), және ол өз орнын еліміздің қазіргі технологиялық құрылымында таба алады. Бұл жағдайдың постанализі еліміздегі IV индустриалқ революцияның жаңа буыны ақпараттық технологияларды құру және ұйымдастырудың маңызды басымдықтарына назар аудару керек деген тұжырымды білдіреді.

Пайдаланылған әдебиеттер тізімі:

1. Токаев К. Повестка дня конференции по разоружению должна быть пересмотрена // Индекс Безопасности. – 2012. – № 1 (100), Том 18. – С.25-30.

2. Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports. https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds/

3. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

4. Developing Story: COVID-19 Used in Malicious Campaigns

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

5. Human hacking: a guide to social engineering

https://www.comtact.co.uk/blog/human-hacking-a-guide-to-social-engineering

6. Европол предупредил о продажах мошенниками некачественных защитных масок

https://tass.ru/obschestvo/8303361

7. Coronavirus update: In the cyber world, the graph has yet to flattenhttps://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/

8. Казахстан вошел в топ-40 стран Глобального индекса кибербезопасности https://zonakz.net/2019/03/29/kazaxstan-voshel-v-top-40-stran-globalnogo-indeksa-kiberbezopasnosti/

References:

1. Tokaev K. Povestka dnya konferencii po razoruzheniyu dolzhna byt' peresmotrena // Indeks Bezopasnosti. – 2012. – № 1 (100), Tom 18. – S.25-30.

2. Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports. https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds/

3. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

4. Developing Story: COVID-19 Used in Malicious Campaigns
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

5. Human hacking: a guide to social engineering
https://www.comtact.co.uk/blog/human-hacking-a-guide-to-social-engineering

6. Evropol predupredil o prodazhah moshennikami nekachestvennyh zashchitnyh masok
https://tass.ru/obschestvo/8303361

7. Coronavirus update: In the cyber world, the graph has yet to flattenhttps://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/

8. Kazahstan voshel v top-40 stran Global'nogo indeksa kiberbezopasnosti https://zonakz.net/2019/03/29/kazaxstan-voshel-v-top-40-stran-globalnogo-indeksa-kiberbezopasnosti/

ҒТАМР 04.51.53 https://doi.org/10.51889/2020-4.1728-8940.27

М.К. Шнарбекова[1], Д.Қ. Мамытқанов[1]*

[1]Қазақ ұлттық университеті,
Алматы, Қазақстан

ЖАС МАМАНДАРДЫҢ ҚАЗАҚСТАННЫҢ ЕҢБЕК НАРЫҒЫНДА КӘСІБИ ҰСТАНЫМДАРЫ

Аңдатпа

Мақалада қазіргі қазақстандық жастардың кәсіби ұстанымдары мен бағыт-бағдарлары жан-жақты талданады. Теориялық тұрғыдан тақырып бойынша талдау нәтижелері ұсынылады. Сонымен қатар, жастар арасында 2018 жылы жүргізілген кешенді әлеуметтанулық зерттеу мәліметті берілген. Зерттеудің жалпы іріктеу көлемі 1000 респондентті құрайды, оның ішінде жас мамандар - 600. Зертеу мәліметтері SPSS for Windows (version 21) лицензиялы бағдарламасымен өңделді.

Мақалада жастардың құндылықтар иерархиясында білім мен жұмыстың орны сараланады. Жастар ортасындағы қалаулы кәсіп бейнесі мен жұмысқа орналасу үшін қажетті талаптар қарастырылады. Сонымен бірге, жас мамандардың өзге салада жұмыс істеу себептерін зерттеу бойынша қорытындылар ұсынылады. Бұл мәселенің қазіргі кезде өзектілігі артуда, себебі кәсіби еңбек нарығын талдау нәтижелері жастардың жоғары оқу орнын аяқтағаннан кейін алғашқы жылдары өз мамандығы бойынша жұмыс істеу көрсеткіштерінің төмендігін айқындайды.

Түйін сөздер: жоғары білім, жастар, білім құндылығы, жастардың кәсіби құндылығы, қалаулы кәсіп бейнесі, кәсіби ұстанымдар.