

АДАМИ ФАКТОРДЫ ЕСКЕРЕ ОТЫРЫП, АҚПАРАТТЫҚ-БІЛІМ БЕРУ ЖҮЙЕЛЕРІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІНІҢ ТӘУЕКЕЛДЕРІН БАҒАЛАУ МОДЕЛІ

АЛЬМУХАНОВА А.К.^{1*}, ЮБУЗОВА Х.И.¹, АЛИМСЕИТОВА Ж.К.¹,
ЛАХНО В.А.²

*Альмуханова Айгерим Казбековна¹ – Докторант, Сәтпаев университеті, Алматы қ., Қазақстан

E-mail: almuhanova_aak@mail.ru, <https://orcid.org/0009-0005-7858-9016>

Юбузова Халича Ибрагимовна¹ – PhD, қауымдастырылған профессор, Сәтпаев университеті, Алматы қ., Қазақстан

E-mail: k.yubuzova@satbayev.university, <https://orcid.org/0000-0001-8892-6745>

Алимсеитова Жұлдыз Кенесхановна¹ – PhD, қауымдастырылған профессор, Сәтпаев университеті, Алматы қ., Қазақстан

E-mail: zh.alimseitova@satbayev.university, <https://orcid.org/0000-0002-1907-8997>

Ляхно Валерий Анатольевич² – Техника ғылымдарының докторы, профессор, Биоресурстар және табиғатты пайдалану ұлттық университеті, Киев қ., Украина.

E-mail: lva964@gmail.com, <https://orcid.org/0000-0001-9695-4543>

Аңдатпа. Мақалада білім беру мекемелерінің ақпараттық-білім беру жүйелерінің (АББЖ) ақпараттық қауіпсіздігінің (АҚ) тәуекелдерін бағалау міндеті қарастырылған. АҚ тәуекелдерін басқарудың қолданыстағы әдістері мен модельдері негізінен корпоративтік және маңызды ақпараттық жүйелердің объектісін қарастыратыны көрсетілген. Бұл модельдер білім беру ортасының ерекшелігін толық ескермейді. Ақпараттық активтер, қауіптер, осалдықтар және пайдаланушылардың мінез-құлық сипаттамалары арасындағы себеп-салдарлық байланыстарды ресімдеуге мүмкіндік беретін Байес желілерінің аппаратына негізделген АҚ тәуекелдерін бағалаудың ықтималдық моделі ұсынылған. Модель статистикалық және сараптамалық деректердің интеграциясын қамтамасыз етеді және оқу орнының мамандарына жүйенің жай-күйі туралы ішінара апарат болған кезде қауіптерді іске асырудың артқы ықтималдығын есептеуге мүмкіндік береді. Адам факторы модельге пайдаланушылардың хабардарлық деңгейін, ақпараттық қауіпсіздік талаптарын сақтауды және олардың мінез-құлқының ерекшеліктерін сипаттайтын байқалатын кездейсоқ айнымалы ретінде енгізілген. Қауіптерді іске асырудың артқы ықтималдығы негізінде күтілетін залал және тәуекелдің интегралды деңгейі анықталады. Ұсынылған тәсілдің өнімділігі білім беру мекемесінің мәліметтеріне есептеу эксперименті арқылы тексеріледі. Рұқсат етілмеген қолжетімділікті, зиянды бағдарламалық қамтамасыз етуді және фишингтік шабуылдарды қоса алғанда, үлгілік ақпараттық активтер және білім беру ортасына тән қауіптер қаралды. Ұсынылған модельдің өнімділігі оқу орнының деректеріндегі есептеу экспериментімен расталады. Эксперимент адам факторының күтілетін зиянға және АҚ интегралды тәуекеліне әсерін талдады. Нәтижелер ұсынылған модельдің мінез құлық параметрлерінің өзгеруіне сезімталдығын көрсетті және оның білім беру мекемелерінің ақпаратын қорғау саласындағы басқарушылық шешімдерді негіздеу үшін практикалық қолданылуын растады.

Түйін сөздер: ақпараттық қауіпсіздік, тәуекелдерді бағалау, ақпараттық-білім беру жүйесі, Байес желілері, адами фактор, күтілетін зиян, білім беру мекемелері.

Кіріспе

Білім беруді цифрландыру жағдайында білім беру мекемелерінің ақпараттық-білім беру ортасы оқу процесінің ажырамас элементіне айналады. Электрондық білім беру ресурстарын, қашықтықтан оқыту жүйелерін (ҚБЖ), корпоративтік желілерді және бұлтты сервистерді пайдалану өңделетін апарат көлемінің өсуіне әкелді. Бұл білім алушылар мен оқу орны қызметкерлерінің дербес деректеріне де қатысты. Тиісінше, білім беру мекемелерінде ақпараттық қауіпсіздікті (АҚ) қамтамасыз етудің маңыздылығы да артып келеді [1; 2].

Білім беру ортасының ерекшелігі [3] ашықтығымен, пайдаланушылардың жоғары таралуымен және адам факторының басым болуымен сипатталады. Бұл, тиісінше, оқу орындарының ақпараттық-білім беру жүйелеріне (АББЖ) қауіп-қатерлер мен осалдықтардың кең ауқымының болуын анықтайды. Қазіргі жағдайда АҚ тәуекелдерін бағалау міндеті өзектілікке ие болды, бұл мамандарға қауіптерді анықтауға, қорғаныс шараларын тандауды негіздеуге және сол арқылы АББЖ киберқорғау дәрежесін арттыруға мүмкіндік береді.

Зерттеу материалдары мен әдістері

АҚ-ны қамтамасыз ету және білім беру мекемелеріндегі тәуекелдерді бағалау мәселелері Covid 19 короновирустық пандемиясы пайда болғанға дейін де зерттеушілердің назарын аударды. Сонымен, [1-4] еңбектерінде авторлар мамандардың иелігіндегі АҚ Басқару модельдері негізінен корпоративті немесе маңызды ақпараттық жүйелерге бағытталған деген тезисті негіздеді. Бұл зерттеулер ақпараттық-білім беру ортасының ерекшелігін толық көрсетпейді. Сондай-ақ, зерттеулердің едәуір бөлігі жоғары оқу орындарының жағдайларына тәуекелдерді басқару стандарттарымен шеңберлерін (ISO/IEC27001, ISO27005, NIST) енгізуге бағытталған. [1; 5; 7; 8; 9] авторлар білім беру ұйымдарында АҚ тәуекелдерін басқару жүйелерін қалыптастырудың өзіндік әдістерін ұсынды. Алайда, бұл әдістер негізінен сараптамалық бағалаулармен сапалышкалаларға сүйенді. АҚ саясатының сәйкестігін және академиялық ақпараттық жүйелердегі қорғаныс жүйелерінің же тілу деңгейін талдауға бағытталған зерттеулер ұқсас сипатта болды [2; 7]. Жеке бағыт ретінде ақпараттық-білім беру жүйелерінің (АББЖ) кибеқауіптері мен осалдықтарын талдаумен байланысты жұмыстарды атап өтеміз. Сонымен, [3; 6; 10] авторлар білім беру мекемелері рұқсатсыз кіруге (NSD), фишингтік шабуылдарға, зиянды бағдарламаларға және пайдаланушылардың қателіктеріне байланысты қауіптердің үстемдігімен сипатталатынын атап өтті. Бұл жағдайда адам факторы тәуекелдің басым көздерінің бірі ретінде белгіленеді. Сонымен қатар, қолданыстағы модельдердің көпшілігінде [1-13] ол жанама түрде немесе сапалы коэффициенттер түрінде ескеріледі. Сондай-ақ, бірқатар авторлар АҚ тәуекелдерін бағалаудың ықтималдық модельдерін ұсынды. Сонымен, [11-13] бастапқы деректердің шектеулі көлеміндегі ықтимал бағалау мен зиянды талдауға негізделген модельдерді қарастырады. Сонымен қатар, бұл модель дер техникалық жүйелерге бағытталған. Олар пайдаланушылардың мінез-құлқының мінез-құлық нюанстарын, сондай-ақ білім беру ортасына тән активтер, қауіптер мен осалдықтар арасындағы күрделі себеп-салдарлық байланыстарды жеткілікті түрде қарастырды.

Жоғарыда айтылғандарға сүйене отырып, бізде АҚ тәуекелдерін бағалаудың қолданыстағы әдістері мен модельдері мен АББЖ жұмысының нақты жағдайлары арасында алшақтық жоқ. Бұл тәуекелдерді бағалаудың интеграцияланған модельдерін әзірлеудің өзектілігін анықтады. Біздің ойымызша мұндай модельдер адам факторының әсерін және АББЖ қа төнетін қауіптердің өзгермелі сипатын ескере алады.

Нәтижелер және оларды талқылау

Зерттеудің мақсаты-активтер, қауіптер мен осалдықтар арасындағы себеп-салдарлық байланыстарды, сондай-ақ адам факторының ақпараттық тәуекелдер деңгейіне әсерін ескеретін ақпараттық-білім беру жүйелерінің ақпараттық қауіпсіздігінің тәуекелдерін бағалаудың ықтималдық моделін әзірлеу және эксперименттік тексеру.

Мақаланың негізгі материалы. Білім беру мекемесінің ақпараттық қауіпсіздік жүйесінің (АҚ) негізгі элементтерінің сипаттамасын енгізейік. Базалық субъектілер ретінде, тиісінше, ақпараттық активтерді, ықтимал қауіптер мен осалдықтарды қарастырыңыз, олардың болуы АҚ инциденттерін іске асару мүмкіндігін анықтайды.

Ақпараттық активтер деп сандық ресурстарды (студенттер мен қызметкерлердің мәліметтер базасы, қашықтықтан оқыту жүйелері, электрондық пошта және т. б.) және ілеспе ақпараттық процестерді түсінеміз. Білім беру ортасының ерекшелігін ескере отырып, көптеген қауіптер мен осалдықтарды қалыптастырамыз. Бұрын [3] көрсетілгендей, соңғысы АББЖ ашықтығының жоғары деңгейімен және айқын адам факторымен сипатталады.

Онда біз АББЖ активтерінің көптігін осылай сипаттаймыз:

$$A = \{A_1, A_2, \dots, A_{NA}, \}, \quad (1)$$

мұнда A_i – i -ақпараттық актив (студенттердің мәліметтер базасы, LMS, пошта, ғылыми репозиторийлер және т. б. , 1-кестені қараңыз).

Кесте 1. Ақпараттық активтер

Активтер		
№	Ақпараттық актив	Қысқашасипаттама
1	Білім алушылардың дербесдеректері.	Жеке басы, үлгерімі, сабаққа қатысуы туралы мәліметтер.
2	Қызметкерлердің дербес деректері.	Кадрлық, байланыс және қызметтік ақпарат.
3	Оқу-әдістемелік материалдар.	Дәрістер, презентациялар, тапсырмалар, тесттер.
4	Оқу нәтижелері.	Бағалар, ведомостар, емтихан нәтижелері.
5	Ғылыми және әдістемелік әзірлемелер.	Мақалалар, есептер, зерттеудеректері.
6	Басқарушылық ақпарат.	Логиндер, парольдер, кіру рөлдері.
7	Пайдаланушының тіркелген деректері.	Логины, пароли, ролі доступа.
8	Электрондық мұрағаттар мен мәліметтер базасы.	Оқу және әкімшілік Ақпарат қоймалары.
Оқу-білім беру мекемесінің техникалық активтері		
9	АББЖ серверлері.	Деректерді сақтау және өңдеу серверлері.
10	Жұмыс станциялары	Оқытушылар мен қызметкерлердің компьютерлері.
11	Білім алушылардың құрылғылары.	Жеке ноутбуктер, планшеттер, смартфондар.
12	Желілік жабдық.	Маршрутизаторлар, қосқыштар, кіру нүктелері
13	Қашықтықтан оқыту жүйелері.	LMS және онымен байланысты бағдарламалық-аппараттық кешендер.
14	Деректерді сақтау жүйелері.	Жергілікті және бұлтты сақтау.
15	Сақтық көшірме жасау құралдары.	Backup үшін серверлермен медиа.
16	Ақпаратты қорғау құралдары.	Брандмауэрлер, антивирустар, бақылау жүйелері.

Кез-келген ақпараттық актив үшін АҚ-ға қатысты көптеген қауіптер бар. Біз тек ең типтік, қандай да бір түрде: білім алушылар мен қызметкерлердің деректеріне рұқсатсыз қол жеткізу (NSD); жеке және Оқу апаратының ағуы; зиянды бағдарламалар мен фишингтік шабуылдар; Оқу материалдары мен оқу нәтижелерін ауыстыру немесе бұрмалау; ОУ АЖ-нің істен шығуы және істен шығуы; электрондық білім беру ресурстарының тұтастығы мен қолжетімділігінің бұзылуы; пайдаланушылардың ережелер туралы хабардар болмауы АҚ.

Тиісінше біз АҚ ның көптеген қауіптерін осылай сипаттаймыз:

$$T = \{T_1, T_2, \dots, T_{NT}, \}, \quad (2)$$

мұнда $A_i - j$ -ші ОУ АЖ қаупі.

Жоғарыда аталған қауіптерді іске асыру оқу орнының АББЖ осалдықтарының болуына байланысты мүмкін болады. Негізгі осалдықтарға АББЖ-да аутентификация мен қол жеткізуді басқарудың әлсіз жүйесі; ескірген бағдарламалық жасақтаманы пайдалану; Желілік және серверлік жабдықты орнатудағы қателер; деректерді үнемі жаңартудың және резервтік көшірудің болмауы; пайдаланушылардың цифрлық сауаттылығының жеткіліксіз деңгейі; АҚ процестерін реттеудің жеткіліксіздігі жатады.

Тиісінше бізде:

$$V = \{V_1, V_2, \dots, V_{Nv}, \}, \quad (3)$$

мұнда $V_k - k$ -шіжүйеніңосалдығы.

Айта кетейік, оқу орындарының АҚ тәуекелдерін бағалау бұлыңғырлыққа тән. Бұл бұлыңғырлыққа келесі себептер әсер етеді: АББЖ активтері мен қауіптерін дәл сипаттауды қиындататын білім беру процестерінің әртүрлілігі мен әлсіз ресімделуі; адами фактор (білім алушылар, оқытушылар, қызметкерлер) мінез-құлықтың жоғары вариациясымен сипатталады; қауіптердің бір бөлігі ықтималды және болжау қиын; қазіргі уақытта АББЖ-дағы АҚ инциденттері бойынша нақты статистика жоқ; сандық емес, сапалық көрсеткіштердің едәуір бөлігі, мысалы, АҚ мәдениеті, бір мәнді өлшеуге жатпайды.

Тиісінше, АҚ тәуекелдерін бағалауға тән бұлыңғырлықты, сондай-ақ толық емес статистикалық және сараптамалық деректерді есепке алу мүмкіндігін есепке алу үшін біз зерттеуге Байес желілерінің (BS) аппаратын қолданамыз. Байес желісі білім беру мекемесінің АББЖ-дағы активтер, қауіптер, осалдықтар мен адам мінез-құлқының факторлары арасындағы себеп-салдарлық байланыстарды математикалық сипаттауға мүмкіндік беру.

Содан кейін АББЖ тәуекелдерін бағалаудың Байес моделі келесідей:

$$B = \langle X, E, P \rangle, \quad (4)$$

мұнда X – кездейсоқайнымалыларжиынтығы; E – ориентированные ағытталғандоғалар, яғнисебептіктәуелділіктер; P – шарттыүлестірімдердіңжиынтығы.

Байес желісі бағытталған ациклді графикпен анықталады. Графиктің түйіндері оқу орнының ақ жүйесі элементтерінің күйін сипаттайтын кездейсоқ айнымалыларға сәйкес келеді. Тиісінше, доғалар олардың арасындағы тәуелділікті көрсетеді. Бұл сандық деректерді бірыңғай ықтималдық моделі шеңберінде сараптамалық бағалаулармен біріктіруге мүмкіндік береді.

Тиісінше, кездейсоқ айнымалылар векторын сипаттайық:

$$X = \{X_A, X_T, X_V, X_H, X_R\}, \quad (5)$$

мұнда X_A – АББЖ активтерінің жай-күйі; X_T – қатерлерді іске асыру; X_V – осалдықтардың болуы; X_H – адам факторы; X_R – тәуекел деңгейі.

Кездейсоқ айнымалылар векторы (5) техникалық параметрлерді де, ұйымдастырушылық және адами факторларды да қамтитынын ескеріңіз. Адам факторын сипаттайтын айнымалыны енгізу білім беру мекемелерінің ерекшелігіне байланысты. [6] мәліметтері бойынша, АҚ инциденттерінің едәуір бөлігі, мысалы, жоғары оқу орындарында, пайдаланушылардың қателіктерімен, хабардарлық деңгейінің жеткіліксіздігімен және АҚ регламенттерінің бұзылуымен байланысты.

Содан кейін BS-де кездейсоқ айнымалылардың ықтималдықтарының бірлескен үлестірімі графиктің құрылымымен анықталған шартты үлестірімдердің көбейтіндісі түрінде ұсынылады. Бұл модельдің есептеу күрделілігін одан әрі азайтуға және жеке қауіптер үшін ықтималдық тұжырымын жүзеге асыруға мүмкіндік береді. Сонымен қатар, АББЖ жағдайы туралы толық емес ақпарат болса да.

$$P(X) = \prod_{i=1}^{|X|} P(X_i | Pa(X_i)) \quad (6)$$

мұнда $Pa(X_i)$ – айнымалының көптеген ата-аналық түйіндері X_i .

Кездейсоқ BS айнымалыларының ықтималдығының бірлескен таралуы графиктің құрылымына сәйкес факторизацияланады. (6) өрнек жүйенің жай-күйі туралы ішінара ақпарат болған кезде ILS үшін жекелеген қауіптерді іске асыру ықтималдығын анықтауға мүмкіндік береді.

Содан кейін АББЖ-да қауіп-қатерді жүзеге асырудың артқы ықтималдығы, есептеулерге сәйкес біз осылай береміз:

$$P(T_j|V_k, H_i) = \frac{P(V_k, H_i|P(T_j))P(T_j)}{P(V_k, H_i)}, \quad (7)$$

мұнда H_i – i -ші адамфакторының жағдайы.

Басқаша айтқанда, АББЖ-да қауіптің кейінгі ықтималдығы (7) бақыланатын факторлар мен жүйе күйлерінің жиынтығы болған жағдайда білім беру мекемесінің АҚ-ның нақты қауіп-қатерінің пайда болуының шартты ықтималдығын білдіреді. Ағымдағы ақпаратты есепке алмай, АББЖ тәуекелінің бастапқы бағасын көрсететін априорлық ықтималдықтан айырмашылығы, біз қосымша мәліметтер негізінде артқы ықтималдықты қалыптастырамыз. Біз бұл деректерді АББЖ жұмыс істеу процесінде аламыз. Деректерді алу үшін операциялық жүйенің журналдары аз қажет. Немесе ОЖ журналдарынан алынған журналдар, антивирустық бағдарламалар және т. б.

Адам факторының жай-күйі, пайдаланушылардың АҚ саласындағы хабардарлығының қандай да бір деңгейі, регламенттерді сақтау, білім алушылар мен қызметкерлердің мінез-құлық ерекшеліктері және басқалары негізгі бақыланатын факторлардың бірі болады. Бұл жағдайдың өзгеруі қауіптердің кейінгі ықтималдығына тікелей әсер етеді. Себебі пайдаланушылардың мінез-құлқы ІУ оқиғаларының ықтималдығын арттыруы да, төмендетуі де мүмкін. Нәтижесінде, артқы ықтималдық (7) адам факторының АББЖ-дағы ақ қауіп-қатер деңгейіне әсерін ескеруге және жаңа өзекті ақпарат болған жағдайда тәуекелді бағалауды нақтылауға мүмкіндік береді.

Әрі қарай, қауіптерді іске асырудың артқы ықтималдығы негізінде біз АББЖ-ның әрбір Ақпараттық активі үшін күтілетін зиянды есептейміз. Бұл АІ оқиғасының дерексіз ықтималдығынан оның салдарын сандық бағалауға көшуге мүмкіндік береді. Соңғысы АББЖ АҚ тәуекелдерін кейінгі талдау үшін қажетті шарт ретінде әрекет етеді.

Жалпы АББЖ активіне күтілетін залалды келесідей береміз:

$$\mathbb{E}[D_i] = \sum_{j=1}^{N_T} P(T_j|A_i) \cdot L_{ij} \quad (8)$$

мұнда $L_{ij} - T_j$ қатері кезінде актив A_i активіне келтірілген залал мөлшері

Интегралды тәуекел жиынтық шама ретінде анықталады. Ол АББЖ үшін қауіпті іске асыру ықтималдығын да, оның тиісті активке әсер ету дәрежесін де ескереді. Алынған тәуекел мәні abb_j ақ күйінің уақыт бойынша өзгеруін сипаттайтын модельдің кіріс параметрі ретінде қолданылады.

$$R_i = \sum_{j=1}^{N_T} P(T_j|A_i) \cdot I_{ij} \quad (9)$$

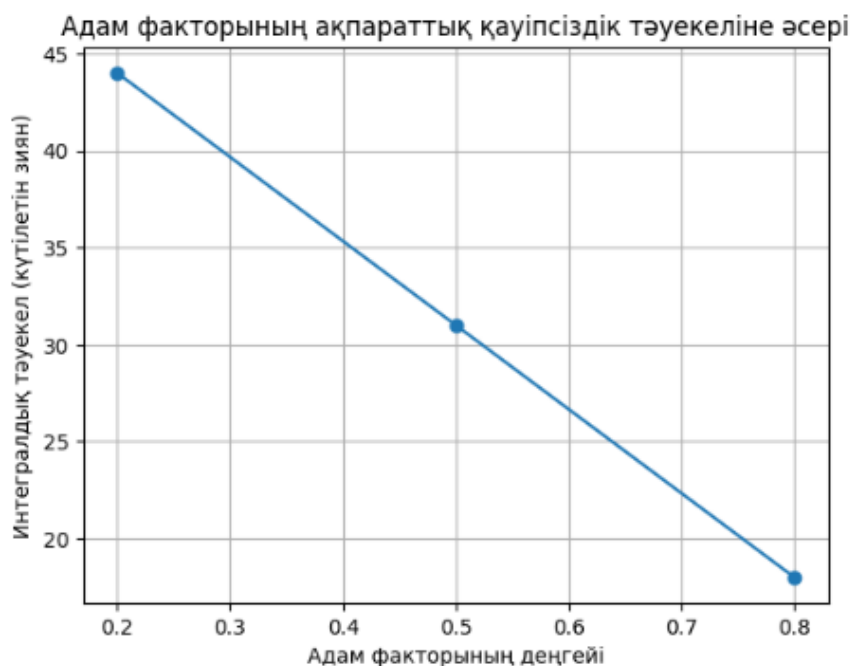
мұнда $I_{ij} - T_j$ қатерінің A_i активіне әсер ету дәрежесі.

АББЖ АҚ тәуекелдерді бағалаудың ұсынылған моделінің жұмысқа қабілеттілігін растау үшін Абай атындағы КНПУ деректерінде есептеу эксперименті жүргізілді. Эксперимент аясында білім беру мекемесінің үш типтік ақпараттық активтері – Дербес деректер (алдын-ала жасырын), қашықтықтан оқыту жүйесі және электрондық пошта және ақпараттық қауіпсіздікке тән үш қауіп қарастырылды: NSD, зиянды бағдарламалар және фишингтік шабуылдар. Аталған қауіптер үшін іске асырудың априорлық ықтималдығы берілген. Олар олардың пайда болуының орташа сараптамалық бағасын көрсетті АББЖ адам факторын есепке алу, модельде (1) – (9) бақыланатын кездейсоқ айнымалы түрінде ұсынылған және 0-ден 1-ге дейінгі мәндерді қабылдаған. Мұнда кішігірім мәндер АҚ талаптарын сақтау мен сақтаудың төмен деңгейіне сәйкес келеді. Ақ мәдениетінің жоғары деңгейіне сәйкес үлкен. Осы фактордың әсерін талдау үшін үш сценарий қарастырылады: адам факторының төмен, орташа және жоғары деңгейі.

Байес қорытындысы негізінде қауіптерді іске асырудың артқы ықтималдығы алынды, олар одан әрі күтілетін залал мен интегралды тәуекелді есептеу үшін қолданылады. Есептеу нәтижелері 2-кестеде және 1 суретте көрсетілген.

Кесте 2. Модельдеу нәтижелері

Адам факторының деңгейі	НСД	Зияндыбағдарлама	Фишинг
0, 2	20, 0	12, 0	12, 0
0, 5	14, 0	8, 4	8, 4
0, 8	8, 0	4, 8	4, 8



Сурет 1. АҚ интегралды тәуекелінің адам факторы деңгейіне тәуелділігі

2-кестеде көріп отырғанымыздай, адам факторы деңгейінің жоғарылауы экспериментте қарастырылған барлық қауіптер бойынша күтілетін залалдың төмендеуіне әкеледі. Нәтиже ұсынылған Модель (1) – (9) шеңберінде мінез-құлық және ұйымдастырушылық аспектілерді есепке алудың дұрыстығын растады.

Қорытынды

Жүргізілген зерттеулер барысында ИБАББЖ тәуекелдерін бағалаудың ықтималдық моделі ұсынылды. Модель Байес желілерін пайдалануға негізделген. Ұсынылған модель ақпараттық активтер, қауіптер, осалдықтар және АҚ инциденттері бойынша бастапқы деректердің шектеулілігі жағдайында адам факторы арасындағы байланысты сипаттауға мүмкіндік берді. Қолданыстағы модельдерден айырмашылығы, ұсынылған модель байқалатын кездейсоқ айнымалы түрінде адам факторын нақты есепке алуды қамтиды. Бұл білім беру мекемелерінің ерекшеліктеріне сәйкес келетіндігі және нәтижесінде АББЖ үшін кибернетикалық қауіптерді жүзеге асыру ықтималдығына пайдаланушылардың хабардарлық деңгейінің және АҚ ережелерін сақтаудың әсерін ескеруге мүмкіндік беретіндігі көрсетілген.

Есептеу экспериментінің нәтижелері адам факторының деңгейінің жоғарылауы күтілетін залалдың төмендеуіне, сондай-ақ қарастырылған барлық қауіптер бойынша интегралды тәуекел деңгейіне әкелетінін растады. Бұл модельдің дұрыстығын растады. Мақалада алынған нәтижелер қолданыстағы зерттеулердегі теориялық алғышарттарға және білім беру жүйелерінің АҚ саласындағы практикалық бақылауларға сәйкес келеді. Ұсынылған модель білім беру мекемелерінің ақпаратты қорғау жүйесін жоспарлау және жетілдіру кезінде шешім қабылдауды қолдау процесінде аналитикалық құрал ретінде пайдалануға жарамды. Сондай-ақ,

көрсетілген модель тәуекелдердің өзгергіштігін есепке алуға және қорғау шараларын тандауды оңтайландыруға бағытталған әрі қарайғы зерттеулер үшін негіз бола алады.

Әдебиеттер тізімі

1. Merchan-Lima J., Astudillo-Salinas F., Tello-Oquendo L., Sanchez F., Lopez-Fonseca G., Quiroz, D. Information security management frameworks and strategies in higher education institutions: a systematic review. // *Annals of Telecommunications*. – 2021. – Vol. 76, no. 3–4. – P. 255–270. – DOI: [10.1007/s12243-020-00783-2](https://doi.org/10.1007/s12243-020-00783-2).
2. Hina S., Dominic P.D.D. Information security policies' compliance: a perspective for higher education institutions. / *Journal of Computer Information Systems*. – 2020. – Vol. 60, no. 3. – P. 201–211. – DOI: [10.1080/08874417.2018.1432996](https://doi.org/10.1080/08874417.2018.1432996).
3. Esparza D.E.I., Diaz F.J., Echeverria T.K.S., Hidrobo S.R.A., Villavicencio D.A.L., Ordonez A.R. Information security issues in educational institutions. // 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). – IEEE, 2020. – P. 1–7. – DOI: [10.23919/CISTI49556.2020.9141014](https://doi.org/10.23919/CISTI49556.2020.9141014).
4. Cheung S.K. Information security management for higher education institutions. // *Intelligent Data Analysis and Its Applications: Proceedings of the First Euro-China Conference on Intelligent Data Analysis and Applications, Shenzhen, China, June 13–15, 2014*. – Cham : Springer International Publishing, 2014. – Vol. 297. – P. 11–19. – DOI: [10.1007/978-3-319-07776-5_2](https://doi.org/10.1007/978-3-319-07776-5_2).
5. Joshi C., Singh U.K. Information security risks management framework – a step towards mitigating security risks in university network. // *Journal of Information Security and Applications*. – 2017. – Vol. 35. – P. 128–137. – DOI: [10.1016/j.jisa.2017.06.006](https://doi.org/10.1016/j.jisa.2017.06.006).
6. Lallie H.S., Thompson A., Titis E., Stephens P. Understanding cyber threats against the universities, colleges, and schools. arXiv:2307.07755. DOI: [10.48550/arXiv.2307.07755](https://doi.org/10.48550/arXiv.2307.07755).
7. Ulinuha Y.K.P., Ayu I.K., Yasmin N.A. Risk assessment maturity level of academic information system using ISO 27001 System Security Engineering–Capability Maturity Model. / *Journal of Applied Engineering and Technological Science*. – 2024. – Vol. 5, no. 2. – P. 941–954. – DOI: [10.37385/jaets.v5i2.2971](https://doi.org/10.37385/jaets.v5i2.2971).
8. Абдыманапов С.А. Методика оценки рисков информационной безопасности на примере анализа Learning Management Systems. // *Вестник Карагандинского университета. Серия «Педагогика»*. – 2022. – Т. 107, № 3. – С. 84–95. – DOI: [10.31489/2022ped3/84-95](https://doi.org/10.31489/2022ped3/84-95).
9. Al-Mudaires F., Al-Samawi A., Aljughaiman A., Nissirat L. Information security risk management framework for a governmental educational institute. // *Journal of Information and Knowledge Management*. – 2023. – Vol. 13, no. 1. – P. 36–54. – DOI: [10.24191/jikm.v13i1.4714](https://doi.org/10.24191/jikm.v13i1.4714).
10. Мулик Д.И., Замотайлова Д.А. Информационная безопасность в учебных заведениях. // *Информационное общество: современное состояние и перспективы развития : материалы международного форума*. – Краснодар : КубГАУ, 2019. – С. 95–98.
11. Воронин Е.А., Козлов С.В., Кубанков А.Н. Выявление угроз на основе ограниченного набора данных при оценке систем обеспечения безопасности и мероприятий по их реализации. // *Наукоемкие технологии в космических исследованиях Земли*. – 2022. – Т. 14, № 3. – С. 41–48.
12. Атаманов А. Н. Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах : дис. ... канд. техн. наук : 05.13.19 / Москва, 2012. – 147 с.
13. Голубинский А.Н., Алехин И.В. О математических моделях ущербов и рисков возникновения угроз в информационно-технических системах. // *Охрана, безопасность, связь*. – 2016. – № 1–3. – С. 109–115.

References

1. Merchan-Lima J., Astudillo-Salinas F., Tello-Oquendo L., Sanchez F., Lopez-Fonseca G., Quiroz, D. Information security management frameworks and strategies in higher education institutions: a systematic review. // *Annals of Telecommunications*. – 2021. – Vol. 76, no. 3–4. – P.

255–270. – DOI: [10.1007/s12243-020-00783-2](https://doi.org/10.1007/s12243-020-00783-2).

2. Hina S., Dominic P.D.D. Information security policies' compliance: a perspective for higher education institutions. / Journal of Computer Information Systems. – 2020. – Vol. 60, no. 3. – P. 201–211. – DOI: [10.1080/08874417.2018.1432996](https://doi.org/10.1080/08874417.2018.1432996).

3. Esparza D.E.I., Diaz F.J., Echeverria T.K.S., Hidrobo S.R.A., Villavicencio D.A.L., Ordonez A.R. Information security issues in educational institutions. // 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). – IEEE, 2020. – P. 1–7. – DOI: [10.23919/CISTI49556.2020.9141014](https://doi.org/10.23919/CISTI49556.2020.9141014).

4. Cheung S.K. Information security management for higher education institutions. // Intelligent Data Analysis and Its Applications: Proceedings of the First Euro-China Conference on Intelligent Data Analysis and Applications, Shenzhen, China, June 13–15, 2014. – Cham : Springer International Publishing, 2014. – Vol. 297. – P. 11–19. – DOI: [10.1007/978-3-319-07776-5_2](https://doi.org/10.1007/978-3-319-07776-5_2).

5. Joshi C., Singh U.K. Information security risks management framework – a step towards mitigating security risks in university network. // Journal of Information Security and Applications. – 2017. – Vol. 35. – P. 128–137. – DOI: [10.1016/j.jisa.2017.06.006](https://doi.org/10.1016/j.jisa.2017.06.006).

6. Lallie H.S., Thompson A., Titis E., Stephens P. Understanding cyber threats against the universities, colleges, and schools. arXiv:2307.07755. DOI: [10.48550/arXiv.2307.07755](https://doi.org/10.48550/arXiv.2307.07755).

7. Ulinuha Y.K.P., Ayu I.K., Yasmin N.A. Risk assessment maturity level of academic information system using ISO 27001 System Security Engineering–Capability Maturity Model. / Journal of Applied Engineering and Technological Science. – 2024. – Vol. 5, no. 2. – P. 941–954. – DOI: [10.37385/jaets.v5i2.2971](https://doi.org/10.37385/jaets.v5i2.2971).

8. Abdymanapov S.A. Metodika ocenki riskov informacionnoj bezopasnosti na primere analiza Learning Management Systems. // Vestnik Karagandinskogo universiteta. Seriya «Pedagogika». – 2022. – T. 107, № 3. – S. 84–95. – DOI: [10.31489/2022ped3/84-95](https://doi.org/10.31489/2022ped3/84-95).

9. Al-Mudaires F., Al-Samawi A., Aljughaiman A., Nissirat L. Information security risk management framework for a governmental educational institute. // Journal of Information and Knowledge Management. – 2023. – Vol. 13, no. 1. – P. 36–54. – DOI: [10.24191/jikm.v13i1.4714](https://doi.org/10.24191/jikm.v13i1.4714).

10. Mulik D.I., Zamotajlova D.A. Informacionnaya bezopasnost' v uchebnyh zavedeniyah. // Informacionnoe obshchestvo: sovremennoe sostoyanie i perspektivy razvitiya : materialy mezhdunarodnogo foruma. – Krasnodar : KubGAU, 2019. – S. 95–98.

11. Voronin E.A., Kozlov S.V., Kubankov A.N. Vyyavlenie ugroz na osnove ogranichennogo nabora dannyh pri ocenke sistem obespecheniya bezopasnosti i meropriyatij po ih realizacii. // Naukoemkie tekhnologii v kosmicheskikh issledovaniyah Zemli. – 2022. – T. 14, № 3. – S. 41–48.

12. Atamanov A. N. Dinamicheskaya iterativnaya ocenka riskov informacionnoj bezopasnosti v avtomatizirovannyh sistemah : dis. ... kand. tekhn. nauk : 05.13.19 / Moskva, 2012. – 147 s.

13. Golubinskij A.N., Alekhin I.V. O matematicheskikh modelyah ushcherbov i riskov vozniknoveniya ugroz v informacionno-tehnicheskikh sistemah. // Ohrana, bezopasnost', svyaz'. – 2016. – № 1–3. – S. 109–115.

МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ С УЧЁТОМ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

АЛЬМУХАНОВА А.К.^{1*}, ЮБУЗОВА Х.И.¹, АЛИМСЕИТОВА Ж.К.¹,
ЛАХНО В.А.²

*Альмуханова Айгерим Казбековна¹ - Докторант, Университет Сатпаева, г. Алматы, Казахстан

E-mail: almuhanova_aak@mail.ru, <https://orcid.org/0009-0005-7858-9016>

Юбузова Халича Ибрагимовна¹ - PhD, ассоциированный профессор, Университет Сатпаева, г. Алматы, Казахстан

E-mail: k.yubuzova@satbayev.university, <https://orcid.org/0000-0001-8892-6745>

Алимсеитова Жулдыз Кенесхановна¹ - PhD, ассоциированный профессор, Университет Сатпаева, г. Алматы, Казахстан

E-mail: zh.alimseitova@satbayev.university, <https://orcid.org/0000-0002-1907-8997>

Лакно Валерий Анатольевич² - Доктор технических наук, профессор, Национальный университет биоресурсов и природопользования, г. Киев, Украина.

E-mail: lva964@gmail.com, <https://orcid.org/0000-0001-9695-4543>

Аннотация. В статье рассмотрена задача оценки рисков информационной безопасности (ИБ) информационно-образовательных систем (ИОС) образовательных учреждений. Показано, что существующие методы и модели управления рисками ИБ в основном рассматривают объект корпоративных и значимых информационных систем. Данные модели не полностью учитывают специфику образовательной среды. Предложена вероятностная модель оценки рисков ИБ, основанная на аппарате байесовских сетей, позволяющая формализовать причинно-следственные связи между информационными активами, угрозами, уязвимостями и поведенческими характеристиками пользователей. Модель обеспечивает интеграцию статистических и экспертных данных и позволяет специалистам учебного заведения рассчитывать обратную вероятность реализации угроз при частичном аппарате о состоянии системы. Человеческий фактор включен в модель как наблюдаемая случайная переменная, характеризующая уровень осведомленности пользователей, соблюдение требований информационной безопасности и особенности их поведения. На основе обратной вероятности реализации угроз определяются ожидаемый ущерб и интегральный уровень риска. Производительность предложенного подхода проверяется расчетным экспериментом на данные образовательного учреждения. Были рассмотрены типовые информационные активы, включая несанкционированный доступ, вредоносное программное обеспечение и фишинговые атаки, а также угрозы, характерные для образовательной среды. Производительность представленной модели подтверждается расчетным экспериментом в данных учебного заведения. Эксперимент проанализировал влияние человеческого фактора на ожидаемый ущерб и интегральный риск ад. Результаты показали чувствительность предложенной модели к изменению параметров поведения и подтвердили ее практическое применение для обоснования управленческих решений в области защиты информации образовательных учреждений.

Ключевые слова: информационная безопасность, оценка рисков, информационно-образовательная система, байесовские сети, человеческий фактор, ожидаемый ущерб, образовательные учреждения.

A MODEL FOR ASSESSING INFORMATION SECURITY RISKS OF INFORMATION AND EDUCATIONAL SYSTEMS BASED ON THE HUMAN FACTOR

ALMUKHANOVA A.K.^{1*}, YUBUZOVA H.I.¹, ALIMSEITOVA ZH.K.¹,
LAKHNO V.A.²

*Almukhanova Aigerim Kazbekovna¹ - Doctoral student, Satbayev University, Almaty, Kazakhstan

E-mail: almukhanova_aak@mail.ru, <https://orcid.org/0009-0005-7858-9016>

Yubuzova Halicha Ibragimovna¹ - PhD, associate professor, Satbayev University, Almaty, Kazakhstan

E-mail: k.yubuzova@satbayev.university, <https://orcid.org/0000-0001-8892-6745>

Alimseitova Zhuldyz Keneskhonovna¹ - PhD, associate professor, Satbayev University, Almaty, Kazakhstan

E-mail: zh.alimseitova@satbayev.university, <https://orcid.org/0000-0002-1907-8997>

Lakhno Valerii Anatolyevich² - Doctor of technical sciences, professor, National university of life and environmental sciences, Kyiv, Ukraine

E-mail: lva964@gmail.com, <https://orcid.org/0000-0001-9695-4543>

Abstract. The article provides for the task of assessing the risks of Information Security (IS) of information and educational systems of educational institutions. It is shown that the existing methods and models of JSC risk management mainly consider the object of corporate and critical information systems. These models do not fully take into account the specifics of the educational environment. A probabilistic model for assessing the risks of JSC based on the Bayesian network apparatus is proposed, which allows formalizing causal relationships between information assets, threats, vulnerabilities and user behavior characteristics. The model provides integration of statistical and expert data and allows specialists of an educational institution to calculate the back probability of implementing threats in the presence of a partial Aparat about the state of the system. The human factor is included in the model as an observable random variable that characterizes the level of awareness of users, compliance with information security requirements and features of their behavior. Based on the posterior probability of implementing threats, the expected damage and the integral level of risk are determined. The performance of the proposed approach is checked by a computational experiment on the data of the educational institution. Model information assets and threats specific to the educational environment, including unauthorized access, malicious software and phishing attacks, were considered. The performance of the presented model is confirmed by a computational experiment in the data of the educational institution. The experiment analyzed the effect of the human factor on the expected harm and the integral risk of white blood cells. The results showed the sensitivity of the presented model to changes in behavioral parameters and confirmed its practical application to justify managerial

Қ.Жұбанов атындағы Ақтөбе өңірлік университетінің хабаршысы, №3 (85), қыркүйек 2026

Компьютерлік ғылымдар-Компьютерные науки-Computer science

decisions in the field of Information Protection of educational institutions.

Key words: information security, risk assessment, information and educational system, Bayesian networks, humanfactor, expected damage, educational institutions.