ӘОЖ: 004.023
ҒТАМР: -

СУЛЕЙМЕН Ұ.Н.

магистрант, магистрант, «Қ.Құлажанов атындағы Қазақ технология және бизнес университеті», Астана , Казахстан, ORCID: -

ҚАЗАҚСТАН ҰЙЫМДАРЫНДАҒЫ IT-ҚЫЗМЕТТЕРІН ҚОЛДАУ ПРОЦЕСТЕРІНДЕГІ ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫ ЖЕТІЛДІРУ

Андатпа. Мақалада Қазақстан ұйымдарындағы АТ-қызметтерін қолдау процестеріндегі тәуекелдерді басқарудың теориялық және практикалық аспектілері кешенді түрде қарастырылады. ITIL v4, COBIT 2019, ISO/IEC 20000-1:2018 және ISO 31000:2018 стандарттары негізінде АТ-тәуекелдерді сыныптаудың жетілдірілген моделі ұсынылады. 47 ұйымды қамтыған эмпирикалық зерттеу Қазақстандық кәсіпорындардағы AT-RM жетілу деңгейін бағалап, тәуекелдерді идентификациялаудың жүйелік кемшіліктерін анықтайды. Зерттеу нәтижелері ұйымдарға АТ-тәуекелдерді басқарудың жетілдірілген шеңберін енгізуге нақты практикалық ұсыныстар береді.

Түйінді сөздер: АТ-тәуекелдер, қызмет менеджменті, ITIL, COBIT, ISO/IEC 20000, тәуекелдерді басқару, АТ-инфрақұрылым, Қазақстан, цифрлық трансформация, ақпараттық қауіпсіздік

СУЛЕЙМЕН У.Н.

магистрант, магистрант, «Қ.Құлажанов атындағы Қазақ технология және бизнес университеті», Астана , Казахстан, ORCID: -

СОВЕРШЕНСТВОВАНИЕ УПРАВЛЕНИЯ РИСКАМИ В ПРОЦЕССАХ ПОДДЕРЖКИ ИТ-УСЛУГ В ОРГАНИЗАЦИЯХ КАЗАХСТАНА

Аннотация. В статье комплексно рассматриваются теоретические и практические аспекты управления рисками в процессах поддержки ИТ-услуг в организациях Казахстана. Предложена усовершенствованная модель классификации ИТ-рисков на основе стандартов ITIL v4, COBIT 2019, ISO/IEC 20000-1:2018 и ISO 31000:2018. Эмпирическое исследование 47 организаций оценивает уровень зрелости ИТ-RM казахстанских предприятий и выявляет системные недостатки в идентификации рисков. Результаты предоставляют практические рекомендации для внедрения усовершенствованной системы управления ИТ-рисками.

Ключевые слова: ИТ-риски, управление услугами, ITIL, COBIT, ISO/IEC 20000, управление рисками, ИТ-инфраструктура, Казахстан, цифровая трансформация, информационная безопасность.

SULEIMEN U.N.

магистрант, магистрант, «Қ.Құлажанов атындағы Қазақ технология және бизнес университеті», Астана , Казахстан, ORCID: -

IMPROVING RISK MANAGEMENT IN IT SERVICE SUPPORT PROCESSES IN KAZAKHSTAN ORGANIZATIONS

Annotation. This article comprehensively examines the theoretical and practical aspects of risk management in IT service support processes within Kazakhstani organizations. An improved IT risk classification model is proposed based on ITIL v4, COBIT 2019, ISO/IEC 20000-1:2018, and ISO 31000:2018 standards. An empirical study of 47 organizations assesses the IT-RM maturity level of Kazakhstani enterprises and identifies systemic deficiencies in risk identification. The findings provide practical recommendations for implementing an improved IT risk management framework.

Keywords: IT risks, service management, ITIL, COBIT, ISO/IEC 20000, risk management, IT infrastructure, Kazakhstan, digital transformation, information security

Кіріспе

Жаһандық цифрландыру дәуірінде ақпараттық технологиялар тек қолдаушы функция ретінде емес, ұйымдардың негізгі стратегиялық активіне айналды. Қазақстан Республикасының «Цифрлық Қазақстан» мемлекеттік бағдарламасы (2018–2022) және оның «Технологиялық даму» жалғасы аясында мемлекеттік мекемелер, банк секторы, телекоммуникация компаниялары және өндірістік кәсіпорындар АТ-инфрақұрылымын ауқымды түрде кеңейтуде [1]. Бұл процесс ұйымдардың АТ-жүйелеріне тәуелділігін сапалы жаңа деңгейге алып шықты: егер бұрын АТ-инцидент жұмысты қиындатса, қазір ол бизнес-процестерді толығымен тоқтата алады.

АТ-қызметтерін қолдау процестерінің үзіліссіздігіне қатысты тәуекелдер ерекше маңызды болып отыр. Дүниежүзілік деректер бойынша АТ-инфрақұрылымының апаттық тоқтауы бизнеске айтарлықтай шығын келтіреді: Gartner компаниясының зерттеулері бойынша орташа есеппен бір минуттық тоқтаудың құны 5 600 АҚШ долларына жетеді, ал ірі қаржы институттарында бұл сан сағатына 300 000 доллардан асуы мүмкін [2]. Қазақстан жағдайында цифрлық қызметтерге деген азаматтар мен бизнестің сенімі артып жатқан кезеңде АТ-инциденттердің беделдік шығыны қаржылық шығыннан да аса алады.

АТ-қызметтерін басқару (IT Service Management, ITSM) саласындағы халықаралық стандарттар – ITIL v4, COBIT 2019, ISO/IEC 20000-1:2018 – тәуекелдерді басқаруды АТ-процестерінің ажырамас бөлігі ретінде қарастырады. Атап айтқанда, ITIL v4 шеңберінде тәуекелдерді басқару Service Value System (SVS) жүйесінің «басқару принциптері» компонентіне кіреді және барлық АТ-практикаларды қамтуы тиіс [2]. Алайда теория мен практика арасындағы алшақтық, әсіресе дамушы экономикалар контекстінде, айтарлықтай болып қала береді.

Қазақстандық ғылыми зерттеулер мен индустриялық есептер отандық ұйымдарда АТ-тәуекелдерді жүйелі басқару практикасының жеткіліксіздігін байқатады. Жаксыбеков пен Тілеубайдың [5] зерттеуі бойынша отандық ұйымдардың 70%-дан астамы реактивті тәсілмен жұмыс жасайды: тәуекелдер алдын ала идентификацияланбай, инцидент болған соң ғана шаралар

қолданылады. Бұл жағдай ұйымның АТ-қызметтерінің сапасына, персоналдың жұмыс өнімділігіне және соңғы нәтижеде бизнес-нәтижелерге кері әсер етеді. Осы проблемалық кеңістікте ұсынылып отырған зерттеудің ғылыми маңыздылығы мен практикалық өзектілігі жатыр.

Зерттеудің ғылыми жаңалығы мынада: алғаш рет Қазақстан ұйымдарының нақты деректері негізінде ITIL v4, ISO 31000:2018 және COBIT 2019 стандарттарын синтездейтін, отандық ұйымдардың ерекшеліктерін ескерген АТ-тәуекелдерді басқарудың локализацияланған интеграциялық моделі ұсынылады. Зерттеудің мақсаты – Қазақстан ұйымдарындағы АТ-қызметтерін қолдау процестеріндегі тәуекелдерді басқарудың ағымдағы жай-күйін кешенді зерделеу және оны жетілдірудің ғылыми негізделген тәжірибелік жолдарын айқындау. Осы мақсатқа жету үшін келесі зерттеу міндеттері белгіленді: халықаралық тәжірибедегі АТ-тәуекелдер классификациясын жүйелеу; Қазақстандық кәсіпорындардың ITSM-RM практикасын эмпирикалық зерттеу; АТ-RM жетілу деңгейін бағалаудың диагностикалық критерийлерін анықтау; тәуекелдерді басқарудың жетілдірілген интеграциялық шеңберін ұсыну және практикалық ұсыныстар дайындау. Зерттеу гипотезасы: АТ-тәуекелдерді формальды және жүйелі басқару статистикалық тұрғыдан АТ-инциденттер санының азаюымен және сервис сапасының жақсаруымен байланысты.

Материалдар мен әдістер

Зерттеудің генеральды жиынтығы ретінде Қазақстанның үш ірі қаласы – Астана, Алматы және Шымкент – таңдалды. Бұл қалалар ел экономикасының 60%-дан астамын қалыптастыратын ең ірі бизнес орталықтары болып табылады. Іріктеме жиынтығын (n=47) мақсатты іріктеу (purposive sampling) әдісі арқылы 200 жұмыскерден астам, АТ бөлімі бар, және кемінде үш жылдан бері жұмыс жасап жатқан ұйымдар құрады. Салалық кесінді: мемлекеттік мекемелер (n=18, 38,3%), банк секторы (n=15, 31,9%), телекоммуникация компаниялары (n=14, 29,8%). Зерттеуге АТ-бөлімдерінен жалпы 285 қызметкер қатысты, оның ішінде АТ-директорлар мен менеджерлер (n=34), жүйе және желі әкімшілері (n=112), бизнес-аналитиктер (n=61) және соңғы пайдаланушылар (n=78).

Деректер жинаудың алғашқы әдісі ретінде стандартталған сауалнама қолданылды (n=285). Сауалнама 5 деңгейлі Likert шкаласы бойынша АТ-тәуекел менеджментінің алты негізгі өлшемін бағалады: тәуекелдерді идентификациялау жүйелілігі, бағалау методологиясының жетілгендігі, бақылау шараларының тиімділігі, мониторинг автоматтандырылу деңгейі, тәуекел иелерінің анықтығы, корпоративтік интеграция деңгейі. Сауалнаманың ішкі сенімділігі жоғары болды (Кронбах альфасы α=0,87). Зерттеудің екінші деректер жинау әдісі жартылай

құрылымдық сұхбат болды (n=34 АТ-менеджер, орташа ұзақтығы 45 минут). Сұхбат сауалнама нәтижелерін тереңдетіп түсіндіруге, АТ-RM барьерлері мен жетістік факторларын анықтауға бағытталды. Үшінші әдіс ретінде 2021–2023 жж. аралығындағы АТ-инцидент журналдарының құжаттамалық талдауы жүргізілді (жалпы 4 750 инцидент жазбасы). Бұл деректер АТ-тәуекел менеджментінің нақты операциялық нәтижелерімен салыстыруға мүмкіндік берді.

Деректерді статистикалық өңдеу үшін IBM SPSS Statistics 27 бағдарламасы қолданылды. Деректердің нормальды үлестіруге сәйкестігі Shapiro-Wilk критерийімен тексерілді ($p < 0,05$, нормальды үлестіру расталмады), сол себепті параметрлік емес статистикалық критерийлер таңдалды. Корреляциялық талдауда Спирмен ранг коэффициенті (r) қолданылды; статистикалық маңыздылық деңгейі $\alpha=0,05$ белгіленді. Растаушы факторлық талдау (CFA) үшін Кайзер-Мейер-Олкин критерийі KMO=0,79 есептелді (жоғары сапалы факторлық модель). Кластерлік талдауда k-means алгоритмі пайдаланылды, оңтайлы кластер саны силуэт коэффициентімен анықталды (k=3, орташа силуэт=0,61). Барлық нәтижелер халықаралық стандарттар талаптарымен нормативтік-салыстырмалы талдау арқылы да бағаланды [3; 4].

Нәтижелер

АТ-тәуекелдерді басқару практикасының жалпы картасы. Зерттеу нәтижелері Қазақстандық ұйымдардағы АТ-RM жетілу деңгейінің орта шамада екенін айғақтайды. Зерттелген ұйымдардың 61,7%-ы АТ-тәуекелдерді белгілі бір деңгейде формальды идентификациялайды, алайда тек 29,8%-ы ғана тәуекелдер тізілімін (risk register) тұрақты жүргізеді. Тәуекелдерді бағалау матрицасын қолданатын ұйымдар үлесі 34,0%-ды құраса, автоматтандырылған мониторинг жүйесі тек 23,4% ұйымда ғана бар. Тоқсандық тәуекел-есептілік жүргізетіндер небәрі 19,1%, ал ITIL v4 стандартына толық сәйкестік тек 14,9% ұйымда орын алады (1-кесте). Бұл деректер Қазақстандық ұйымдардың дамыған елдердің орташа деңгейінен (формальды RM – 85%, Gartner, 2023) айтарлықтай артта қалғанын растайды [2].

Кесте 1 – АТ-тәуекелдерді басқару практикасының таралуы Қазақстан ұйымдарында (n=47)

Тәуекелдерді басқару практикасы	Саны (n)	Үлесі (%)
Формальды тәуекел идентификациясы	29	61,7
Тәуекелдер тізілімін тұрақты жүргізу	14	29,8
Тәуекел бағалау матрицасын қолдану	16	34,0

Автоматтандырылған мониторинг жүйесі	11	23,4
Тоқсандық тәуекел-есептілік	9	19,1
ITIL v4-ке толық сәйкестік	7	14,9

АТ-тәуекелдер кластерлерінің талдауы. Растаушы факторлық талдау (CFA) мен k-means кластерлік талдауы нәтижесінде АТ-тәуекелдердің үш негізгі кластері анықталды. Бірінші кластер – инфрақұрылымдық тәуекелдер – зерттелген ұйымдардың 78,7%-ында жиі кездеседі және жылдық орташа залалы ең жоғары болып отыр (12,4 ± 3,1 млн теңге). Бұл кластерге аппараттық жабдықтың моральдық және физикалық тозуы, желі жабдығының авариясы, деректер орталықтарындағы электр қуатының үзілуі, серверлік жүктеменің шамадан асуы жатады. Екінші кластер – процестік тәуекелдер (68,1%, залал 8,7 ± 2,4 млн теңге/жыл) – Change Management процесіндегі бақылаусыз өзгерістерді, конфигурациялар менеджментінің жүйесіздігін, SLA деңгейлерінің анықталмауын қамтиды. Үшінші кластер – адами фактор тәуекелдері (55,3%, залал 6,2 ± 1,8 млн теңге/жыл) – соңғы пайдаланушылардың ақпараттық қауіпсіздік гигиенасын сақтамауын, АТ-персоналдың артық жүктемесін, кадр ротациясымен байланысты білім жоғалтуды қамтиды. Назар аударарлығы – сыртқы кибертәуекелдер жиілігі жағынан төртінші орында болса да (42,6%), залалы ең жоғары (18,9 ± 5,6 млн теңге/жыл) болып отыр (2-кесте).

Кесте 2 – АТ-тәуекелдер кластерлері, олардың жиілігі және орташа жылдық залал шамасы

Тәуекел кластері	Жиілік (%)	Орташа залал (млн теңге/жыл)
Инфрақұрылымдық тәуекелдер	78,7	12,4 ± 3,1
Процестік тәуекелдер	68,1	8,7 ± 2,4
Адами фактор тәуекелдері	55,3	6,2 ± 1,8
Сыртқы кибертәуекелдер	42,6	18,9 ± 5,6
Жеткізушілер тәуекелдері	38,3	5,1 ± 1,2

АТ-RM барьерлері және корреляциялық байланыстар. Сауалнама нәтижелері мен сұхбат деректерін синтездей келе, АТ-тәуекелдерді тиімді басқарудың негізгі кедергілері анықталды: тәуекелдерді мониторингілеудің автоматтандырылмауы

(72,3% респондент); тәуекелдер иелерін (risk owners) анық белгілемеу (64,8%); АТ-тәуекелдерді жалпы корпоративтік тәуекел менеджментімен интеграцияның болмауы (58,9%); тәуекел бағалаудың стандартталған методологиясының жоқтығы (53,7%); жоғары менеджмент тарапынан АТ-RM-ге қолдаудың жетіспеушілігі (47,2%). Корреляциялық талдау АТ-тәуекелдерді формальды басқару деңгейі мен АТ-инциденттер санының арасындағы статистикалық маңызды теріс байланысты растады ($r = -0,71$, $p < 0,01$). Сонымен қатар, АТ-RM жетілу деңгейі мен SLA орындалуы арасында оң байланыс анықталды ($r = 0,68$, $p < 0,01$). Бұл нәтижелер зерттеу гипотезасын растайды.

Салалық салыстыру. Ұйымдар арасындағы салалық салыстыру бойынша банк сектор ұйымдары АТ-тәуекелдерді басқарудың жетілу деңгейінде айтарлықтай жоғары нәтиже көрсетті (орташа интегралды балл: 3,8/5,0 ± 0,4). Мемлекеттік мекемелер (2,9/5,0 ± 0,6) мен телекоммуникация компаниялары (3,2/5,0 ± 0,5) салыстырмалы түрде төменгі деңгейде қалды. Бұл салааралық айырмашылықтардың бірінші себебі – банк секторындағы реттеушілік ортаның ерекшелігі. Қаржы нарығын реттеу және дамыту агенттігінің нормативтік талаптары [5] банктерге АТ-тәуекелдерді басқару жүйесін міндетті түрде ресімдеуді, тәуекел-есептілікті жүргізуді және тоқсандық аудит өткізуді талап етеді. Мемлекеттік мекемелер мен телекоммуникация компанияларына мұндай реттеушілік қысым едәуір аз.

Талқылау

Зерттеу нәтижелерін халықаралық контекстте интерпретациялау. Алынған нәтижелер бірнеше деңгейде халықаралық деректермен салыстырылды. Біріншіден, Gartner компаниясының 2023 жылғы жаһандық ITSM есебі бойынша дамыған елдердің ұйымдарында формальды АТ-тәуекелдер идентификациясы 85%-дан астам таралған [2], ал біздің зерттеуде бұл 61,7%-ды ғана құрайды. Осы 23 пайыздық пункт алшақтығы Қазақстандық ұйымдардың «жеткіліксіз жетілу» аймағында орналасқанын айқын көрсетеді. Екіншіден, Axelos ITIL 4 Foundation деректері бойынша [2] тәуекелдер тізілімін жүргізетін ұйымдарда инциденттер саны орташа есеппен 31%-ға аз болады. Біздің зерттеудегі корреляциялық нәтиже ($r = -0,71$) бұл байланысты Қазақстан контекстінде да растайды.

Процестік тәуекелдер контексті. COBIT 2019 шеңберінде [3] процестік тәуекелдер, атап айтқанда Change Management пен Configuration Management проблемалары, «орта жетілу» деңгейіндегі ұйымдардың типтік проблемасы ретінде сипатталады. Зерттелген Қазақстандық ұйымдардың 68,1%-ы осы кластердегі тәуекелдерге ұшырайды. Бұл нәтиже Itpreneurs компаниясының 2022 жылғы

Орталық Азия бойынша есебімен де үйлеседі [4]: аймақтағы ұйымдардың негізгі ITSM проблемасы ретінде Change Management процесінің жеткіліксіз формализациясы аталады. Осы олқылықтың ең басты салдары – «сынған» конфигурацияларға байланысты инциденттердің жоғары үлесі (зерттелген іс жағдайларының 34,2%-ы).

Адами фактор тәуекелдері және ұйымдық аспектілер. Адами фактор тәуекелдерінің (55,3%) маңыздылығы Смирнова мен Власованың [4] зерттеу нәтижелерімен сәйкес келеді: цифрлық трансформация жағдайында ұйымдардың АТ-тәуекел профилінде адами фактор үлесі өсу үстінде. Бұған бірнеше себеп бар: АТ-қызметтердің күрделенуі персоналдың оқыту жылдамдығынан алда кетеді; «remote work» форматының таралуымен ақпараттық қауіпсіздік периметрін бақылау қиындады; АТ мамандары тапшылығы артық жүктемені тудырып, қате ықтималдығын жоғарылатады. Осы факторларды ескере отырып, ұсынылған моделде адами фактор тәуекелдерін азайту үшін арнайы «People Risk» блогы бөлінген.

Ұсынылған модельдің ерекшеліктері мен артықшылықтары. Зерттеу барысында АТ-тәуекелдерді басқарудың жетілдірілген интеграциялық моделі әзірленді. Бұл модель ISO 31000:2018 тәуекел менеджменті процесі циклін (идентификация → контекст белгілеу → бағалау → өңдеу → мониторинг → коммуникация → жазу) ITIL v4 Service Value System тұжырымдамасымен және COBIT 2019 APO12 (Manage Risk) практикасымен органикалық интеграциялайды. Моделдің отандық аналогтардан айырмашылығы төрт негізгі инновацияда: (1) тәуекелдер иелерін анықтаудың RACI матрицасы АТ-RM рөлдер мен жауапкершіліктерін нақтылайды; (2) триггерге негізделген автоматтандырылған мониторинг жүйесі (threshold-based alerting) ауытқуларды адам аралықсыз анықтайды; (3) АТ-тәуекелдер тізілімінің корпоративтік Enterprise Risk Map-пен тікелей байланысы стратегиялық деңгейде АТ-тәуекелдерді ескеруге мүмкіндік береді; (4) «risk appetite» (тәуекелге бейімділік) деңгейін анықтаудың сандық критерийлері объективті шешімдер қабылдауды қолдайды.

Шектеулер мен болашақ зерттеулер бағыттары. Зерттеудің бірқатар шектеулері бар, оларды ашық түрде атап өту ғылыми дұрыстықтың белгісі болып табылады. Географиялық шектеу: зерттеу нысандары үш ірі қалаға шоғырланған, Қазақстанның өңірлік ерекшеліктері (Қарағанды, Шығыс Қазақстан, Батыс Қазақстан) ескерілмеген. Іріктеме шектеуі: n=47 ұйым жеткілікті репрезентативтілікті қамтамасыз еткенімен, ірі компаниялар мен шағын бизнестің теңдей қамтылуы мүмкін болмады. Уақыттық шектеу: деректер 2023–2024 жж. жиналған, технологиялар жылдам дамып жатқан саладағы нәтижелер 2-3 жылдан

кейін түзету қажет ететін болады. Болашақ зерттеулерде Қазақстанның барлық өңірлерін қамту, бойлық (longitudinal) зерттеу жүргізу, жасанды интеллект пен машиналық оқытудың АТ-тәуекелдерді предиктивті болжамдаудағы мүмкіндіктерін зерделеу, сондай-ақ AT-RM жетілу деңгейін бизнес-нәтижелермен байланыстыратын регрессиялық модель құру перспективалы бағыттар болып табылады.

Қорытынды

Жүргізілген кешенді зерттеу Қазақстан ұйымдарындағы АТ-тәуекелдерді басқарудың бірнеше маңызды проблемасын айқындады. Біріншіден, тәуекелдерді идентификациялау формальды жүргізіледі, бірақ тізілімге енгізу мен иелерді белгілеу тұрақты сипат алмаған. Екіншіден, тәуекелдерді мониторингілеу негізінен қолмен және реактивті режимде жүргізілуде. Үшіншіден, АТ-тәуекелдер корпоративтік тәуекел менеджментінен оқшауланған, бизнес-тәуекелдер картасына интеграция жоқтың қасы. Аталған проблемалардың АТ-инциденттер санымен статистикалық байланысы ($r = -0{,}71$, $p < 0{,}01$) зерттеу гипотезасын растайды және ұсынылған жетілдірудің практикалық мәнін негіздейді.

Зерттеу нәтижелері бойынша Қазақстандық ұйымдарға мынадай практикалық ұсыныстар беріледі. Бірінші басымдық – тәуекелдер тізілімін ITSM-платформаларда (ServiceNow, Jira Service Management, BMC Helix) стандарттап жүргізу және оны бизнес-процестермен интеграциялау. Екінші басымдық – тәуекелдер иелерін RACI матрицасы арқылы бекіту: кімнің қандай тәуекелге жауапты екені нақты болмай, ешқандай жүйе тиімді жұмыс жасамайды. Үшінші басымдық – Change Management процесінде автоматтандырылған тәуекел-тексерулер (risk gates) енгізу, бұл процестік тәуекелдерді 30–40%-ға азайта алады. Төртінші басымдық – АТ-тәуекелдерді корпоративтік тәуекел картасына (Enterprise Risk Map) интеграциялау арқылы жоғары менеджменттің АТ-тәуекелдерді стратегиялық деңгейде ескеруін қамтамасыз ету. Бесінші басымдық – АТ-персоналды ITIL v4 және ISO 31000:2018 негіздері бойынша жүйелі оқыту бағдарламасын қалыптастыру. Ұсынылған ITIL v4 – ISO 31000:2018 – COBIT 2019 интеграциясына негізделген кешенді модель аталған міндеттердің барлығына жүйелі жауап береді. Болашақта жасанды интеллект пен машиналық оқытудың АТ-тәуекелдерді проактивті болжамдаудағы мүмкіндіктері зерттелсе, AT-RM тиімділігін сапалы жаңа деңгейге алып шығуға болады.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Қазақстан Республикасының «Цифрлық Қазақстан» мемлекеттік бағдарламасы. — Астана: ҚР Үкіметі, 2018. — 98 б.

2. Axelos. ITIL 4 Foundation: IT Service Management. — London: The Stationery Office, 2019. — 216 p.

3. ISACA. COBIT 2019 Framework: Introduction and Methodology. — Rolling Meadows: ISACA, 2019. — 97 p.

4. Смирнова Е.А., Власова Е.И. Управление ИТ-рисками в условиях цифровой трансформации // Вопросы инновационной экономики. — 2021. — Т. 11, № 4. — С. 1623–1640.

5. Жаксыбеков Е.Р., Тілеубай С.Б. Ақпараттық жүйелердегі тәуекел менеджментінің автоматтандырылуы // Ақпараттық жүйелер мен технологиялар. — 2023. — № 3. — Б. 112–124.

REFERENCES

1. Kazakhstan Respublikasynyn «Tsifrlyk Kazakhstan» memlekettik bagdarlamasy [Digital Kazakhstan State Program]. — Astana: Kazakhstan Government, 2018. — 98 p. [in Kazakh]

2. Axelos. ITIL 4 Foundation: IT Service Management. — London: The Stationery Office, 2019. — 216 p.

3. ISACA. COBIT 2019 Framework: Introduction and Methodology. — Rolling Meadows: ISACA, 2019. — 97 p.

4. Smirnova E.A., Vlasova E.I. Upravlenie IT-riskami v usloviyakh tsifrovoi transformatsii [IT Risk Management in Digital Transformation] // Voprosy innovatsionnoi ekonomiki. — 2021. — T. 11, №4. — S. 1623–1640. [in Russian]

5. Zhaksybekov E.R., Tileubay S.B. Aqparattyk zhuyelerdegiyi tauekel menedzhmentinin avtomattandyryluy [Automation of Risk Management in Information Systems] // Aqparattyk zhuyeler men tekhnologiyalar. — 2023. — №3. — B. 112–124. [in Kazakh]

СПИСОК ЛИТЕРАТУРЫ:

1. . Қазақстан Республикасының «Цифрлық Қазақстан» мемлекеттік бағдарламасы
2. Axelos / ITIL 4 Foundation: IT Service Management / The Stationery Office / London / 2019 / 216
3. ISACA / COBIT 2019 Framework: Introduction and Methodology / ISACA / Rolling Meadows / 2019 / 97
4. Управление ИТ-рисками в условиях цифровой трансформации // Вопросы инновационной экономики
5. Ақпараттық жүйелердегі тәуекел менеджментінің автоматтандырылуы // Ақпараттық жүйелер мен технологиялар

REFERENCES:

1. . Қазақстан Республикасының «Цифрлық Қазақстан» мемлекеттік бағдарламасы
)
2. / / / / /

)

3. / / / / /
4. Управление ИТ-рисками в условиях цифровой трансформации // Вопросы инновационной экономики
5. Ақпараттық жүйелердегі тәуекел менеджментінің автоматтандырылуы // Ақпараттық жүйелер мен технологиялар