QAZAQ JOURNAL OF YOUNG SCIENTIST

2026, Vol.4, No. 4 S (April)

https://qazaqjournal.kz/

ӘОЖ **657.6:004**

ҰЙЫМДАҒЫ IT АУДИТІНІҢ ТИІМДІЛІГІН БАҒАЛАУ

Жақып А.Қ.
«IT менеджменті» ғылыми-педагогикалық бағдарламасының магистранты,
Қ.Құлажанов атындағы Қазақ технология және бизнес университеті,
Ақпараттық технологиялар кафедрасы, Астана қ.

Ғылыми жетекші: Ламашева Ж.Б., PhD, доцент

Бұл мақалада Қазақстан Республикасындағы инфокоммуникация саласын дамытудың негізгі институты - «Зерде» ұлттық инфокоммуникациялық холдингі» АҚ мысалында IT аудит жобасын әзірлеу қарастырылады. Холдинг АКТ активтерін басқарады және электрондық үкімет пен IT инфрақұрылымын дамытуды қоса алғанда, мемлекеттік цифрлық жобаларды іске асыруға қатысады. Сандық тәуекелді бағалауды, метрика жүйесін және қауіптерді басымдыққа бөлу моделін қамтитын ресми AT аудит әдіснамасы ұсынылады. IT инфрақұрылымы үшін тәуекелді бағалау кестелері және интеграцияланған қауіпсіздік индексі моделі әзірленді.

Кілт сөздер: IT аудиті, тәуекелдерді басқару, ақпараттық қауіпсіздік, COBIT, ISO 27001, цифрландыру, Зерде.

«Зерде» ұлттық инфокоммуникациялық холдингі» АҚ – Қазақстан Республикасындағы ақпараттық-коммуникациялық технологиялар саласындағы негізгі мемлекеттік даму институты. Холдинг мемлекеттік IT активтерін басқаруды орталықтандыру, сондай-ақ экономика мен мемлекеттік басқаруды цифрландыру саласындағы стратегиялық бастамаларды үйлестіру және жүзеге асыру үшін құрылған.

Компанияның қызметі мемлекеттік ақпараттық жүйелер мен қызметтердің тұрақты жұмыс істеуін қамтамасыз ететін заманауи цифрлық инфрақұрылымды құруға және дамытуға бағытталған. Холдингтің маңызды бағыты – оның халық

пен бизнес үшін мемлекеттік қызметтердің қолжетімділігі мен сапасын жақсартуға ықпал ететін электрондық үкіметті құру мен дамытуға қатысуы.

Холдинг ақпараттық жүйелерді әзірлеуге, енгізуге және қолдауға, сондай-ақ телекоммуникация және бұлтты инфрақұрылымды дамытуға қатысатын бірқатар ұйымдарды біріктіреді. Оның қызметіне әртүрлі цифрлық шешімдерді біріктіру, инновациялық технологияларды енгізу және мемлекеттік деңгейде IT ресурстарын басқару тиімділігін арттыру кіреді.

«Зерде» АҚ өңделетін деректердің жоғары маңыздылығы мен инфрақұрылымының ауқымына байланысты ақпараттық қауіпсіздікке ерекше назар аударады. Ақпараттық қауіпсіздікті, жүйенің сыртқы және ішкі қауіптерге төзімділігін және халықаралық стандарттарға сәйкестігін қамтамасыз ету холдингтің басты басымдықтары болып табылады.

Осылайша, «Зерде» Ұлттық инфокоммуникация холдингі» АҚ Қазақстанның цифрлық трансформациясының негізгі элементі ретінде қызмет етеді, АКТ секторының дамуын қамтамасыз етеді, үкіметтің цифрлық бастамаларын қолдайды және елдің технологиялық тәуелсіздігін арттырады.

ҚР мемлекеттік басқаруы мен экономикасын цифрландыру үшін жоғары сенімді АТ инфрақұрылымы қажет. Осыған байланысты «Зерде» Ұлттық инфокоммуникация холдингі» АҚ АКТ экожүйесінің дамуын және оның АТ еншілес компанияларын басқаруды қамтамасыз ететін негізгі рөл атқарады. Архитектураның күрделілігі және өңделген деректердің маңызды сипаты сандық талдау әдістерін қолдана отырып, үнемі АТ аудиттерін жүргізуді қажет етеді.

Зерттеу мақсаты: Тәуекелдерді бағалаудың формальды модельдерін қолдана отырып, АТ аудит жобасын әзірлеу.

АТ аудитінің теориялық моделі. АТ аудитінің теориялық моделі басқару, тәуекелдер, қауіпсіздік және белгіленген стандарттарға сәйкестік арасындағы өзара байланысқа негізделген ұйым ішіндегі ақпараттық технологиялардың жай-күйін бағалаудың жүйелі тәсілін білдіреді. Бұл модель шеңберінде АТ аудиті бір реттік шолу ретінде емес, корпоративтік басқару жүйесіне интеграцияланған үздіксіз процесс ретінде қарастырылады.

Теориялық IT моделі аудитінің бірнеше негізгі компоненттерге тәуелді функция ретіндегі тұжырымдамасына негізделген: IT басқару деңгейі, тәуекел дәрежесі, ақпараттық қауіпсіздік деңгейі және нормативтік сәйкестік. Бұл элементтер үнемі өзара әрекеттеседі және ұйымның IT ортасының жалпы жағдайын қалыптастырады.

IT басқару ақпараттық жүйелердің стратегиялық бағытын және олардың бизнес мақсаттарымен сәйкестігін анықтайды. Тиімді IT басқару процестердің ашықтығын, жауапкершілікті тағайындауды және IT ресурстарын пайдалануды бақылауды қамтамасыз етеді. Тәуекел деңгейлері, өз кезегінде, ақпараттық

жүйелердің жұмысына байланысты жағымсыз оқиғалардың ықтималдығын, сондай-ақ оларды енгізуден болатын ықтимал залалды көрсетеді.

Ақпараттық қауіпсіздік деректердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған қорғаныс механизмі ретінде әрекет етеді. Оған жүйенің осалдығын азайтатын және ықтимал қауіптердің әсерін азайтатын техникалық және ұйымдастырушылық шаралар кіреді. Модельдің негізгі элементі - IT басқару және ақпараттық қауіпсіздік саласындағы халықаралық стандарттар сияқты стандарттар мен нормативтік талаптарға сәйкестік, бұл IT процестерінің сапасын бағалауға және жақсартуға бірыңғай тәсілді қолдануға мүмкіндік береді.

Теориялық модельдің орталығында сандық және сапалық әдістерді қолдану арқылы жүзеге асырылатын тәуекелді бағалау жатыр. Тәуекел жүйенің осалдық деңгейі мен қолданыстағы бақылау шараларының тиімділігін ескере отырып, қауіптің пайда болу ықтималдығы мен ықтимал залалдың шамасының көбейтіндісі ретінде қарастырылады. Бұл тәсіл тек маңызды салаларды ғана емес, сонымен қатар басқару шешімдеріне басымдық береді.

Сонымен қатар, IT моделі инфрақұрылымының жалпы жағдайын бағалау үшін интеграцияланған индикаторларды пайдаланады. Бұған ұйым үшін маңыздылығына қарай жеке тәуекелдерді біріктіру арқылы қол жеткізіледі. Нәтижесінде IT жүйелерін жетілдіру бойынша ұсыныстар әзірлеу үшін қолданылатын тұтас көрініс пайда болады.

Осылайша, IT аудитінің теориялық моделі ақпараттық технологияларды басқарудың тиімділігін арттыруға, тәуекелдерді азайтуға және сандық трансформация жағдайында ұйымның тұрақты жұмыс істеуін қамтамасыз етуге бағытталған кешенді талдау және бағалау жүйесін білдіреді.

IT аудиті келесі функциялардың бірі ретінде қарастырылады:

$$ITA=f\,(G,R,S,C) \qquad (1)$$

мұндағы:
G – IT басқару деңгейі;
R – тәуекел деңгейі;
S – қауіпсіздік деңгейі;
C – стандартқа сәйкестік.

АТ аудитіндегі тәуекелдерді бағалау әдіснамасы ұйымның ақпараттық жүйесінің тұрақтылығы мен қауіпсіздігіне әсер етуі мүмкін ықтимал қауіптерді анықтауға, талдауға және сандық бағалауға бағытталған бірізді және құрылымдалған процесс болып табылады. Бұл процесс АТ аудитінің негізгі элементі болып табылады, себебі ол АТ инфрақұрылымын жақсарту және осалдықтарды азайтудың басым бағыттарын анықтауға мүмкіндік береді.

Бірінші кезең ақпараттық жүйелердің жұмысымен байланысты ықтимал қауіптер мен осалдықтарды анықтауды қамтитын тәуекелдерді анықтауды қамтиды. Тәуекел көздеріне кибершабуылдар, рұқсатсыз кіру және зиянды бағдарламалар сияқты сыртқы факторлар, сондай-ақ адами қателіктер, кіруді бақылау кемшіліктері және ескірген бағдарламалық жасақтама сияқты ішкі факторлар кіруі мүмкін. Бұл кезең сонымен қатар дерекқорлар, сервер инфрақұрылымы және корпоративтік ақпараттық жүйелер сияқты маңызды активтерді анықтайды.

Келесі кезең - әрбір тәуекелдің орын алу ықтималдығын және ол келтіруі мүмкін ықтимал залалды бағалайтын тәуекелдерді талдау. Ықтималдық жағымсыз оқиғаның жиілігін немесе ықтималдығын көрсетеді, ал залал қаржылық шығындарды, жүйенің бұзылуын және беделге нұқсан келтіретін тәуекелдерді қоса алғанда, бизнес-процестерге теріс әсер ету дәрежесін сипаттайды. Талдаудың дәлдігін арттыру үшін жүйенің қауіптерге ұшырауын көрсететін осалдық деңгейі және қолданыстағы бақылау шараларының тиімділігі қосымша ескеріледі.

Сандық тәуекелді бағалау формальды модельді қолдану арқылы жүзеге асырылады, онда тәуекел оқиғаның ықтималдығының, оның әсерінің, осалдық деңгейінің және бақылау тиімділігінің кері шамасының көбейтіндісі ретінде анықталады. Бұл тәсіл тәуекелдерді сандық бағалауға және оларды салыстыруға мүмкіндік береді, талдаудың объективтілігі мен ашықтығын қамтамасыз етеді.

Сандық бағалаудан кейін тәуекелдерді саралау кезеңі орындалады, оның барысында анықталған тәуекелдер маңыздылық деңгейі бойынша төменнен сыни деңгейге дейін жіктеледі. Бұл одан әрі әрекеттерге басымдық беруге және ресурстарды ең қауіпті салаларға шоғырландыруға мүмкіндік береді. Тәуекел матрицасы бұл кезеңде маңызды құрал болып табылады, ол бағалау нәтижелерін визуализациялауға және шешім қабылдау процесін жеңілдетуге мүмкіндік береді.

Әдістеменің соңғы кезеңі - тәуекелдерді басқару шараларын әзірлеу. Тәуекелдің маңыздылығына байланысты әртүрлі стратегиялар қолданылуы мүмкін, соның ішінде қосымша қауіпсіздік шараларын енгізу, беру (мысалы, сақтандыру), қабылдау немесе толық жою арқылы азайту. Аутентификация, мониторинг және резервтік көшірме жүйелері сияқты қолданыстағы бақылау құралдарының тиімділігін арттыруға ерекше назар аударылады.

Осылайша, IT аудитіндегі тәуекелдерді бағалау әдіснамасы сәйкестендіруді, талдауды, сандық бағалауды және тәуекелдерді басқаруды біріктіретін кешенді процесс болып табылады. Оны қолдану ақпараттық жүйелердің тұрақтылығын арттырады, оқиғалардың ықтималдығын азайтады және сандық ортада басқару шешімдерін қабылдауға негіз болады.

Негізгі тәуекел формуласы. Классикалық модель қолданылады:

$$Risk_i = P_i \cdot Impact_i \quad (2)$$

мұндағы:
Pi - қауіптің пайда болу ықтималдығы;
$Impact_i$ - залал.

АТ аудитіндегі кеңейтілген тәуекел моделі қауіпті бағалауға тереңірек және кешенді тәсілді білдіреді, ол тек оқиғалардың ықтималдығы мен салдарын ғана емес, сонымен қатар ақпараттық жүйенің ішкі сипаттамаларын және қолданыстағы қорғаныс шараларының тиімділігін ескереді. Бұл модель жеңілдетілген бағалаудан дәлірек және негізделген тәуекел талдауына көшуге мүмкіндік береді, бұл әсіресе дамыған және маңызды АТ инфрақұрылымы бар ұйымдар үшін маңызды.

Тәуекел оқиғаның ықтималдығы мен залалдың шамасының көбейтіндісі ретінде анықталатын негізгі модельден айырмашылығы, кеңейтілген модель жүйенің нақты жағдайын көрсететін бірқатар факторлармен толықтырылады. Ең алдымен, ол ақпараттық жүйенің ықтимал қауіптерге ұшырау дәрежесін сипаттайтын осалдық деңгейін ескереді. Осалдық ескірген бағдарламалық жасақтама немесе жаңартулардың болмауы сияқты техникалық кемшіліктермен, сондай-ақ әлсіз қолжетімділік саясаты мен қызметкерлерді оқытудың жеткіліксіздігі сияқты ұйымдастырушылық мәселелермен байланысты болуы мүмкін.

Кеңейтілген модельдің тағы бір маңызды элементі - қолданыстағы қорғаныс шараларының тиімділігін көрсететін бақылау деңгейі. Бұл шараларға аутентификация, мониторинг, антивирустық қорғау, резервтік көшірме жасау және қолжетімділікті басқару жүйелері кіреді. Бақылау деңгейі неғұрлым жоғары болса, соғұрлым тәуекел төмен болады, себебі тиімді қорғаныс механизмдері қауіптің сәтті болу ықтималдығын азайтады немесе оның салдарын азайтады.

Осы факторларды ескере отырып, кеңейтілген модельдегі тәуекел қауіптің пайда болу ықтималдығының, ықтимал залалдың, осалдық деңгейінің және басқару тиімділігінің функциясы ретінде анықталады. Бұл ұйымның IT ортасындағы нақты жағдайды дәлірек көрсетуге және басымдықты қажет ететін маңызды салаларды анықтауға мүмкіндік береді.

Сонымен қатар, кеңейтілген модель қауіп нысанаға алған активтің маңыздылығы және оқиғаларды анықтау жылдамдығы сияқты параметрлерді қарастыра алады. Маңыздылық активтің ұйымның жұмыс істеуі үшін маңыздылығын көрсетеді, ал анықтау жылдамдығы салдардың ауқымына әсер етеді, себебі оқиғаларды уақтылы анықтау зиянды азайтуға көмектеседі. Бұл

факторларды қосу модельді белгілі бір ұйымның нақты қажеттіліктеріне икемді және бейімделгіш етеді.

Осылайша, IT аудитіндегі кеңейтілген тәуекел моделі техникалық және ұйымдастырушылық қауіпсіздік аспектілерін қарастыруға мүмкіндік беретін көп факторлы талдау құралын білдіреді. Оны пайдалану тәуекелді дәлірек сандық бағалауға мүмкіндік береді, шешімдердің жарамдылығын жақсартады және киберқауіптердің артуына байланысты IT инфрақұрылымын тиімді басқаруға ықпал етеді.

Кеңейтілген тәуекел моделі (IT аудиті үшін)

$$Risk_i = P_i \cdot Impact_i \cdot V_i \cdot (1 - C_i) \quad (3)$$

мұндағы:

V_i – осалдық деңгейі (0–1);

C_i – бақылау деңгейі (қорғаныс тиімділігі).

«Зерде» холдингі үшін практикалық іске асыру. IT инфрақұрылымының ерекшеліктері. «Зерде» ұлттық инфокоммуникация холдингі» АҚ үшін IT аудит жобасын практикалық іске асыру оның IT инфрақұрылымының ерекшеліктерін ескеруді қамтиды, ол өте күрделі, ауқымды және мемлекеттік қызметтердің жұмыс істеуі үшін маңызды. Бұл инфрақұрылымның ерекшеліктері көбінесе аудит тәсілін, тәуекелдерді бағалау әдістерін таңдауды және ұсыныстар әзірлеуді анықтайды.

Біріншіден, холдингтің IT инфрақұрылымы таратылған. Оған ішкі корпоративтік шешімдерден бастап ұлттық цифрлық платформаларға дейін әртүрлі деңгейлерде жұмыс істейтін әртүрлі еншілес компаниялар мен ақпараттық жүйелер кіреді. Бұл әртүрлі жүйелерді біріктіруді және олардың үйлесімділігін қамтамасыз етуді қажет етеді, бұл өз кезегінде басқару мен мониторингтің күрделілігін арттырады.

Маңызды ерекшелік - негізгі IT ресурстарын орталықсыздандыру кезінде олардың жұмысын жоғары деңгейде орталықтандырылған басқару. Орталық басқару органдары даму стратегиясын, стандарттарын және қауіпсіздік саясатын анықтайды, ал жеке бөлімшелер немесе еншілес компаниялар нақты жүйелерді енгізу және қолдау үшін жауапты. Бұл модель бірыңғай стандарттар мен тиімді үйлестіру механизмдерін қатаң сақтауды талап етеді.

Холдингтің IT инфрақұрылымы деректер орталықтары, бұлтты платформалар, үкіметтік дерекқорлар және электрондық үкімет қызметтері сияқты көптеген компоненттерді қамтиды. Үлкен көлемдегі деректерді өңдеу және олардың нақты уақыт режимінде қолжетімділігін қамтамасыз ету жүйенің жұмысына, ақауларға төзімділікке және масштабталуға жоғары талаптар қояды.

Ақпараттық қауіпсіздік деңгейі ерекше маңызды. Холдинг азаматтардың жеке деректері мен мемлекеттік органдардың деректерін қоса алғанда, маңызды мемлекеттік ақпаратты өңдейтіндіктен, ақпараттық қауіпсіздік талаптары коммерциялық ұйымдарға қарағанда айтарлықтай жоғары. Бұған көп деңгейлі қауіпсіздік жүйелерін пайдалану, үздіксіз қауіп-қатерді бақылау және халықаралық стандарттарға сәйкестік қажеттілігі кіреді.

Қосымша ерекшелік - бизнес-процестердің IT жүйелерінің тұрақтылығына жоғары тәуелділігі. Кез келген ақаулар немесе оқиғалар тек қаржылық шығындарға ғана емес, сонымен қатар мемлекеттік қызметтердің үзілуіне де әкелуі мүмкін, бұл инфрақұрылымның сенімділігі мен тұрақтылығын басымдыққа айналдырады.

Осылайша, «Зерде» холдингінің IT инфрақұрылымы өзінің таралуымен, масштабымен, жоғары интеграция дәрежесімен және өңделген деректердің маңыздылығымен сипатталады. Бұл сипаттамалар сандық бағалау әдістеріне және заманауи ақпараттық қауіпсіздікті басқару құралдарына негізделген IT аудитіне кешенді және тәуекелге негізделген тәсілді талап етеді.

«Зерде» ұлттық инфокоммуникациялық холдингі келесі сипаттамалармен сипатталады:

• таратылған құрылым (компаниялар тобы);
• электрондық үкімет жобаларына қатысу;
• ұлттық IT ресурстарын басқару.

1-кесте. Активтерді анықтау

№	Активтер	Белсенді сыни көзқарас (1–5)
1	Мемлекеттік дерекқорлар	5
2	Деректерді өңдеу серверлері	5
3	Бұлттық инфрақұрылым	4
4	Тұтыну жүйелері	3

2-кесте. Тәуекелді бағалау матрицасы

Қауіп	P	Impact	V	C	Risk
Деректердің ағып кетуі	0.6	5	0.8	0.4	1.44
Кибершабуыл (DDoS)	0.7	4	0.7	0.5	0.98
Инфрақұрылымның істен шығуы	0.5	5	0.6	0.6	0.6
Адам факторы	0.8	3	0.9	0.3	1.51

«Зерде» Ұлттық инфокоммуникациялық холдингі» АҚ IT инфрақұрылымының тиімділігі мен тұрақтылығын арттыру үшін біз

техникалық, ұйымдастырушылық және басқару деңгейлерін қамтитын бірқатар ұсыныстар ұсынамыз.

Техникалық деңгейде ақпараттық жүйелерге кіруді қорғау механизмдерін күшейту басты назарда. Осыған байланысты, тіркелгі деректері бұзылған жағдайда да рұқсатсыз кіру ықтималдығын айтарлықтай азайтатын көп факторлы аутентификацияны енгізу ұсынылады. Сонымен қатар, оқиғаларды нақты уақыт режимінде жинайтын, өзара байланыстыратын және талдайтын, оқиғаларды жедел анықтауға және алдын алуға мүмкіндік беретін орталықтандырылған қауіпсіздік оқиғаларын бақылау және талдау (SIEM) жүйелерін енгізуді ұсынамыз. Бағдарламалық жасақтаманы үнемі жаңартуды және қауіпсіздік патчтарын уақтылы қолдануды қамтамасыз ету де маңызды, бұл осалдықтарды азайтады және белгілі қауіптерді пайдалану қаупін азайтады.

Ұйымдастыру шаралары ұйым ішінде тұрақты ақпараттық қауіпсіздік мәдениетін қалыптастыруға бағытталған. Негізгі элемент - қызметкерлерді заманауи киберқауіптер және ақпараттық жүйелермен қауіпсіз жұмыс істеу ережелері туралы хабардар етуге бағытталған үнемі оқыту. Адами қателіктер оқиғалардың ең көп таралған себептерінің бірі болып қала береді, сондықтан қызметкерлердің құзыреттілігін арттыру жалпы тәуекел деңгейін айтарлықтай төмендетеді. Сонымен қатар, деректерге қол жеткізуді, өңдеуді және сақтауды, сондай-ақ оқиғаларға жауап беру рәсімдерін реттейтін кешенді ақпараттық қауіпсіздік саясатын әзірлеу және енгізу қажет.

Басқару деңгейінде тәуекелге негізделген АТ басқару моделіне көшу ұсынылады, онда барлық басқару шешімдері тәуекелдерді және олардың ұйымның қызметіне ықтимал әсерін бағалау негізінде қабылданады. Бұл тәсіл ресурстарды тиімдірек бөлуге және ең маңызды салаларға назар аударуға мүмкіндік береді. Маңызды қадам - халықаралық басқару және қауіпсіздік стандарттарын, әсіресе COBIT және ISO/IEC 27001 интеграциялау. Оларды бірлесіп қолдану АТ процестерін басқаруға жүйелі тәсілді қамтамасыз етеді, ашықтықты арттырады, процедураларды стандарттайды және АТ инфрақұрылымының жоғары деңгейдегі жетілуіне ықпал етеді. Осылайша, ұсынылған ұсыныстар АТ ортасының қауіпсіздігін, басқарылуын және тиімділігін арттыруға бағытталған кешенді шаралар жүйесін құрайды, бұл әсіресе жоғары сандық жүктеме және маңызды ақпаратты өңдеу жағдайында жұмыс істейтін ұйымдар үшін маңызды.

Пайдаланылған әдебиеттер тізімі

1. Белых Н.В., Кашин Д.В., Демина Т.Ю. Ұйымдастырушылық ақпараттық жүйелердегі деректер сапасын бағалаудың IT аудиті // Басқару есебі. - 2024. № 2.

2. Скляренко С.С. Ақпараттық технологиялар аудиті: оқу құралы. - Мәскеу: INFRA-M, 2023. 212 б.

3. Крамер Д.А. Ішкі бақылау мен аудиттің тиімділігін бағалау // Халықаралық гуманитарлық және жаратылыстану ғылымдары журналы. 2021. № 5-3. 153-156 б.

4. Игибаева З.К. АТ аудитінің әдіснамалық негіздері және Қазақстан Республикасында АКТ пайдалану саласындағы мемлекеттік органдардың тиімділігін бағалау // Ғылыми журнал. 2026. (COBIT 2019 және ISO/IEC 27001 стандарттары бойынша ағымдағы зерттеулер).

5. Смайылов А. А., Ахметов Р. С. және т.б. Қазақстан Республикасындағы мемлекеттік аудит: оқулық. - Астана: Зерттеу, талдау және тиімділікті бағалау орталығы, 2025. 424 б.

6. Мұхамедьярова Л. Р., Тусибаева Г. С. Қазақстан Республикасы ұйымдарында IT аудитін жүргізудің ұйымдастырушылық және құқықтық аспектілерін бағалау // ҚазТБУ хабаршысы. 2025. № 3.

7. Әлімбеков А. Б. Қазақстанда IT аудитін енгізу және жетілдіру // Тұран университетінің хабаршысы. 2023. № 2. 118-125 бб.

8. Кухаренко Е. В. IT жобаларын енгізудің тиімділігі: бағалау әдістері және тәуекелдері // Қарағанды университетінің хабаршысы. 2022.

ОЦЕНКА ЭФФЕКТИВНОСТИ ИТ-АУДИТА В ОРГАНИЗАЦИИ

Жақып Ә.К.

Научный руководитель: Ламашева Ж.Б., PhD, асисстент профессора

В статье рассматривается разработка проекта ИТ-аудита на примере АО «Национальный инфокоммуникационный холдинг «Зерде» - ключевого института развития инфокоммуникационной отрасли Республики Казахстан. Холдинг выполняет функции управления ИКТ-активами и участвует в реализации государственных цифровых проектов, включая развитие электронного правительства и ИТ-инфраструктуры. Предложена формализованная методика ИТ-аудита, включающая количественную оценку рисков, систему метрик и модель приоритизации угроз. Разработаны таблицы оценки рисков, а также модель интегрального индекса безопасности ИТ-инфраструктуры.

Ключевые слова: ИТ-аудит, управление рисками, информационная безопасность, COBIT, ISO 27001, цифровизация, Зерде.

ASSESSING THE EFFECTIVENESS OF AN IT AUDIT IN AN ORGANIZATION

Zhaqyp A.K.

Supervisor: Lamasheva Zh.B., PhD, Assistant Professor

This article examines the development of an IT audit project using the example of JSC "National Infocommunication Holding "Zerde" - a key institution for the development of the infocommunications industry in the Republic of Kazakhstan. The holding manages ICT assets and participates in the implementation of state digital projects, including the development of e-government and IT infrastructure. A formalized IT audit methodology is proposed, including a quantitative risk assessment, a metrics system, and a threat prioritization model. Risk assessment tables and an integrated security index model for the IT infrastructure have been developed.

Keywords: IT audit, risk management, information security, COBIT, ISO 27001, digitalization, Zerde.

REFERENCES

1. Belykh, N.V., Kashin, D.V., Demina, T.Yu. IT Audit of Data Quality Assessment in Organizational Information Systems. Management Accounting, 2024, No. 2.
2. Sklyarenko, S.S. Audit of Information Technologies: Textbook. — Moscow: INFRA-M, 2023. — 212 p.
3. Kramer, D.A. Evaluation of the Effectiveness of Internal Control and Audit. International Journal of Humanities and Natural Sciences, 2021, No. 5-3, pp. 153–156.
4. Igibayeva, Z.K. Methodological Foundations of IT Audit and Evaluation of the Effectiveness of Public Authorities in the Use of ICT in the Republic of Kazakhstan. Scientific Journal, 2026. (Based on current studies in COBIT 2019 and ISO/IEC 27001 standards).
5. Smayilov, A.A., Akhmetov, R.S., et al. Public Audit in the Republic of Kazakhstan: Textbook. — Astana: Center for Research, Analysis and Performance Evaluation, 2025. — 424 p.
6. Mukhamedyarova, L.R., Tusibayeva, G.S. Assessment of Organizational and Legal Aspects of Conducting IT Audit in Organizations of the Republic of Kazakhstan. Bulletin of Kazakh University of Technology and Business, 2025, No. 3.
7. Alimbekov, A.B. Implementation and Improvement of IT Audit in Kazakhstan. Bulletin of Turan University, 2023, No. 2, pp. 118–125.
8. Kukharenko, E.V. Efficiency of IT Project Implementation: Evaluation Methods and Risks. Bulletin of Karaganda University, 2022.