ОӘЖ 004.222

УНИВЕРСИТЕТТІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН БАҒАЛАУ ӘДІСТЕМЕСІН ӘЗІРЛЕУ

Кемербаева Райхангүл Қайратқызы
k.raikhan97@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан
Ғылыми жетекшісі – т.ғ.к., доцент м.а. Омарбекова А.С.

Аннотация.Ақпараттық қауіпсіздік тәуекелдерін бағалау ақпараттық жүйеде қауіпсіздікті жобалаудың маңызды бөліктерінің бірі болып табылады. Ұйымдар ақпараттық активтерді және олармен байланысты қауіпсіздік тәуекелдерін жүйелі және жан-жақты анықтау үшін ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін қолданады. Бұл мақалада ақпараттық активтерді қорғау және анықтау туралы негізгі ұғымдар талданады.

Түйінді сөздер: ақпараттық қауіпсіздік, тәуекел, осалдықтар, әдістеме, актив.

1. КІРІСПЕ

Ақпараттық қауіпсіздік тәуекелдерін басқару әдістемелері бұл ұйымдар өздерінің ақпараттық активтерін жүйелі түрде анықтап, белсенді қорғауға және сол арқылы материалдық және материалдық емес шығындарды азайтуға мүмкіндік беретін құрал болып табылады.Ақпараттық қауіпсіздік тәуекелдерін бағалауды зерттеуде қолдануға болатын көптеген құралдар мен әдістер бар.Соның ішінде ақпараттық қауіпсіздік тәуекелінің сандық көрсеткіштерін анықтауға негізделген ақпараттық қауіпсіздік тәуекелдерін бағалаудың әдісін қарастырамыз. Әдістеменің негізгі міндеті ақпаратты қорғау бойынша тиімді шаралар қабылдау мақсатында ақпарттық қауіпсіздік тәуекелінің сандық көрсеткішін анықтау болып табылады. Әдістеме ISO/IEC27001:2013 халықаралық стандартына сәйкес ақпараттық қауіпсіздік басқару жүйесінің шеңберінде ақпараттық ресурстардың құпиялылығын, дербестігін, тұтастығын және қолжетімділігін кез келген бұзу негізінде тәуекелдерді сәйкестендіру, бағалау және өңдеу процесін айқындайды. Бұл құжат ақпараттық қауіпсіздік тәуекелдеріне және ақпараттық тәуекелдерді басқару процесіне, сондай-ақ кез-келген байланысты рөлдерге, міндеттерге және қызметке қатысты әдіснаманың негізгі принциптерін сипаттайды.[1]

2. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН БАҒАЛАУ ӘДІСТЕМЕСІНІҢ СИПАТТАМАСЫ

Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі мынадай кезеңдерден тұрады:

I. кезең. Активтерді сәйкестендіру;

II. кезең. Қауіп-қатер моделін әзірлеу;

III. кезең.Тәуекелдерді бағалау.

2.1. I КЕЗЕҢ. АКТИВТЕРДІ СӘЙКЕСТЕНДІРУ

Ақпараттық қауіпсіздік тәуекелдерін бағалаудың бірінші кезеңінде университеттің ақпараттық активтерін сәйкестендіру жүзеге асырылады. Пайдаланылатын активтерді анықтау мақсатында ақпараттық қауіпсіздік басқару жүйесінің қолданылу аясына кіретін университеттің әр бөлімінің/қызметінің қызметкерлерімен сұхбат жүргізіледі.

2.1.1. Ақпараттық активтер тізілімін жасау

Жүргізілген талдау нәтижелері бойынша университет активтерін санаттарға бөлу қағидаларына/нұсқаулығына сәйкес активтер тізілімі жасалады.

2.1.2. Активтердің иелерін анықтау

Анықталған ақпараттық активтер үшін активтердің иелері анықталады. Ақпараттық активтердің иелері-нақты маңызды ақпараттық активтерді қорғауға жауапты адамдар (қызметтер/бөлімдер/департаменттер). Меншік иелері ақпараттық қауіпсіздік тапсырмаларын

менеджерлерге немесе басқаларға тапсыра алады, бірақ олар тапсырмалардың дұрыс орындалуына өздері жауап береді.

2.1.3. Ақпараттық ресурстардың құпиялылық (C), тұтастық(I), қол жетімділк (A), дербес(P) және үздіксіздік(U) деңгейін анықтау

Әрбір ақпараттық актив CIAPU параметрлері бойынша бағаланады. CIAPU сандық түрде есептеледі және әр активке ұпай беру арқылы қойылады. Құпиялылық, тұтастық және қол жетімділік деңгейлері келесі шекаралармен анықталады:

Кесте 1. CIAPU параметрлерін бағалау

Атрибут атауы	Мәні	Коэффициент
Құпиялылығы (C)	Иә	0.2
	Жоқ	0
Тұтастық (I)	Иә	0.2
	Жоқ	0
Қол жетімділік (A)	Сирек	0.075
	Күнделікті	0.15
	Жиі	0.2
Дербес (P)	Иә	0.2
	Жоқ	0
Үздіксіздік(U)	Иә	0.2
	Жоқ	0

2.1.4 Сақтау атрибуттарын анықтау

Әрбір анықталған ақпараттық актив үшін ақпараттық ресурстарды сақтаудың мынадай атрибуттары бойынша бірқатар мәндер айқындалады:

	Атрибут атауы	Мәні
	Кем дегенде бір компьютерде сақталуы	Иә
		Жоқ
	Активті мәліметтер базасынан табуға болады ма?	Иә
		Жоқ
	Актив қағаз түрінде бар ма?	Иә
		Жоқ
	Активтісақтау/беруүшінтасымалданатынақпараттасығыштарпайдаланылады ма?	Иә
		Жоқ
	Дербес деректердің болуы	Иә
		Жоқ

2.1.5 Санаттау және жіктеу

Ақпараттық активтерді санаттаудың мақсаты ақпараттың құпиялылық режимін қамтамасыз ету жөніндегі заңнамалық және ішкі нормативтік құжаттардың талаптарын қанағаттандыру болып табылады. Ақпараттық активтерді санаттау келесі құпиялылық дәрежесінде жүзеге асырылады:

Кесте 3. Ақпаратты жіктеу

	Категория	Сипаттамасы
	Қызметтік	Құжаттардың әртүрлі түрлеріндегі, сондай-ақ қызметтік функцияларды орындау процесінде алынатын қызметтік сипаттағы мәліметтер.
	Құпия	Ұйымның операциялық және қаржы-шаруашылық қызметіне қатысты деректер. Құпия ақпараттың толық тізімін "университеттің құпия ақпаратының тізімі"-нен қараңыз.
	Таратылуы шектеулі ақпарат	Ұйымдардың қызметіне қатысты құпия емес ақпарат, оларды таратуға шектеулер қызметтік қажеттіліктен туындаған, қол жетімділігі шектеулі ақпарат.

2.1.6 Ақпараттың таралып кетуінен / ашылуынан болуы мүмкін бедел тәуекелдерінің деңгейін айқындау.

Университеттің ақпараттық активтеріне жүргізілген түгендеу барысында тәуекел деңгейінің келесі жіктемесіне сәйкес ақпаратты жария еткен жағдайда ұйымға келтірілген зиянның ықтимал мөлшері келесідей белгіленеді:

Кесте 4. Шығын мөлшерін жіктеу

Шығын мөлшері	Сипаттамасы	Коэффициент
Өте төмен	Материалдық шығын жоқ, қызметкерлер мен пайдаланушылар тарапынан ең аз мөлшерде наразылық.	1
Төмен	Шығын материалдық емес, қызметкерлер мен пайдаланушылардың сенім деңгейінің аздап төмендеуі.	2
Орташа	Шығын материалдылықтан аз, қызметкерлер мен пайдаланушылар тарапынан сенім деңгейінің төмендеуі, ең аз көлемде реттеуші санкциялар қолданылуы.	3
Жоғары	Айтарлықтай шығын материалдылықтан көп, пайдаланушылардың /серіктестердің белгілі бір бөлігінің сенімін жоғалту, компания туралы теріс ақпараттың тарауы, реттеуші санкциялар, сот шығындары.	4
Апаттық	Банкроттықжәнежұмыстытоқтату, беделгеқалпынакелтірілмейтінзалал, пайдаланушылар/серіктестертарапынантолықсенімжоғалтужәнекомпанияменжұмысістеуденбастарту, сотқудалауы, маңыздыреттеушісанкциялар.	5

2.1.7 Тәуекелдің туындау ықтималдығын анықтау

Университеттің ақпараттық активтерінің иелерімен сұхбат жүргізу барысында тәуекелдің туындау ықтималдығының келесі жіктелуіне сәйкес тәуекелдің туындау ықтималдығы белгіленеді:

Кесте 5. Тәуекел ықтималдығын жіктеу

Тәуекелдің пайда болу ықтималдығы	Сипаттамасы	Коэффициент
Өте төмен	Екіталай	1
Төмен	Үш жылда бір рет	2
Орташа	Жылына бір рет	3
Жоғары	Жылына бірнеше рет	4
Өте жоғары	Айына бір рет және одан көп	5

2.2. II КЕЗЕҢ. ҚАУІП-ҚАТЕР МОДЕЛІН ӘЗІРЛЕУ

Бұл кезеңде бағалау қолайсыз оқиғалардың туындау ықтималдығы мен олардың өзектілігін анықтауды ескере отырып, негізгі қауіптердің моделі әзірленеді.Талдау жүргізу барысында осы қатерлерге ұшыраған активтердің әрбір сәйкестендірілген тобына өзекті қатерлердің тізбесі жасалады.

2.3.III кезең.Тәуекелдерді бағалау

Сәйкестендірілген тәуекелдердің сандық шамасын анықтау үшін есептеу келесі алгоритмге сәйкес жүзеге асырылады:

1. CIAPU атрибуттары бойынша активтердің салмағын есептеу;
2. Келтірілген зиян шамасының салмағын есептеу.
3. Берілген классификацияға сәйкес тәуекелдің ықтималдығын есептеу.
4. Әрбір актив үшін тәуекелдің бағалау көрсеткішінің жиынтық балын мынадай формула бойынша есептеу:

$$\text{Тәуекелді бағалау} = \frac{\text{Ықтималдық} * \text{Шығын мөлшері} * (\text{C} + \text{I} + \text{A} + \text{P} + \text{U})}{25} * 100$$

Бұл ретте тәуекелдің ең жоғары жол берілетін мәні 25 балл болуы мүмкін екенін атап өткен жөн, яғни **(5*5*(0.2+0.2+0.2+0.2+0.2) = 25),** тәуекелдіа бағалау нәтижелері түсіндірудің ыңғайлылығы үшін пайызбен көрсетіледі.

5. Тәуекелдің бағалау көрсеткішінің орташа балын есептеу келесі формула бойынша есептеледі:

$$\text{Орташа бал} = \frac{\sum_{N}^{1} \text{Әрбір актив тәуекелінің бағалау көрсеткіші}}{N},$$

Мұндағы N - осы қауіпке ұшыраған сәйкестендірілген активтердің саны.

6. Тәуекелдің рұқсат етілген көрсеткішін анықтау.

Кесте 7. Тәуекел аймақтары

Диапазон	**Тәуекел аймағы**	**Мәні**
>=15 балов	**Рұқсатетілген тәуекел аймағы**	Тәуекелдіңрұқсатетілгендеңгейінеұйымныңқызметінеәсеріжоқнемесеазәсерететінақпараттықтәуекелдержатады.
<15 балов	**Сыни аймақ**	Ұйымныңқызметінеәсеретуіайтарлықтайзиянкелтіруімүмкінақпараттықтәуекелдерсынитәуекелдераймағынатүседі.

3. ҚОРЫТЫНДЫ

Тәуекелдерді басқару процесі- басшылыққа шешім қабылдауға көмектесетін бизнес-процесс. Бұл активтерді басқарушыларға кәсіпорын активтерін қорғау бойынша өз міндеттерін дұрыс және мұқият орындауға мүмкіндік береді. Процесс ұзаққа созылмауы керек. Тиімді болу үшін тәуекелдерді талдау және бағалау тез және сапалы жүргізілуі керек.

Әдісті қолдану оңай, ол дәстүрлі әдістерге қарағанда есептеулерді аз қажет етеді. Бұл әдіс кірістерге сезімталдықты, күрделілікті және ақпараттық қауіпсіздік тәуекелдерін бағалаудың басқа да мәселелерін болдырмайды. Сонымен қатар, практикалық нәтижелерге қарап әдістің артықшылығын көруге болады.Тәуекелдерді тиімді басқару процесінің мақсаты бақылау құралдарын қажет болған жағдайда ғана енгізу болып табылады.Ұйым активтерін анықтай білу және қандай қауіп-қатерлер бар екенін және қандай кепілдіктер бар екенін анықтау мүмкіндігі кез-келген ұйымның шектеулі ресурстарын пайда әкелетін жаққа бағыттауды қамтамасыз етеді.[2]

Тәуекелдерді бағалау кез-келген ұйымды сәтті басқарудың маңызды құрамдас бөлігі болып табылады. Бұл жоба басталғаннан басталып, бағдарлама, жүйе аяқталғанша және күтілетін артықшылықтар орындалғанға дейін жалғасатын процесс. Тәуекелдерді бағалау кез келген жаңа немесе өсіп келе жатқан тәуекелдерді анықтау үшін жобаның басқа салаларын тұрақты мониторинг жүргізе отырып, ең үлкен тәуекел салаларына бағытталуы керек.

Қолданылған әдебиеттер тізімі

1. Shedden, P., Ahmad, A., Smith, W., Tscherning, H., … Scheepers, R. (2016). Asset Identification in Information Security Risk Assessment: A Business Practice Approach. Communications of the Association for Information Systems, 39, 297–320.

2. Talabis, M., & Martin, J. (2012). Information Security Risk Assessment: Risk Assessment. Information Security Risk Assessments, 147–175.