ОӘЖ 004.056

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН ТАЛДАУ ЖӘНЕ БАҒАЛАУ

Егембердиева Нурсулу Амирханқызы
namirkhanovna@gmail.com
Толыкбаева Айлина Ганиевна
ailina16@mail.ru
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Ақпараттық технологиялар факультеті
Информатика және ақпараттық қауіпсіздік кафедрасының магистранттары,
Нұр-Сұлтан, Қазақстан

Қауіпсіздік тақырыбы өте кең және адамның әр түрлі күнәларына қатысты көптеген мәселелерді қамтиды. Қауіпсіздік - бұл оған құқығы жоқ пайдаланушылардың қашықтағы қызметтерге қол жеткізуге талпыныстарының жолын кесу.

Қауіпсіздік мәселелерінің көпшілігі өздеріне пайда келтіруге немесе басқаларға зиян келтіруге тырысатын зиянкестерден туындайды. Алғашқы жақындау кезінде желілік қауіпсіздік мәселелерін төрт бірдей аймаққа бөлуге болады: құпиялылық, аутентификация, қатаң сәйкестік және тұтастық. Қауіпсіздік тақырыбы өте кең және көптеген мәселелерді қамтиды. Құпиялық (құпиялылық) дегеніміз ақпараттың рұқсат етілмеген пайдаланушылардың қолына түсуіне жол бермеуді білдіреді.

Тәуекелдерді бағалау процесінің мақсаты –ақпаратқа қатысты тәуекел сипаттамалары жүйесінің (IP) және оның ресурстарын (активтер) анықтау. Алынған мәліметтер негізінде қажетті қорғаныс құралдарын таңдауға болады. Тәуекелдерді бағалау кезінде көптеген факторлар ескеріледі: ресурстардың құндылығы, қауіптер мен осалдықтардың маңыздылығын бағалай отырып, қолданыстағы және жоспарланған емдеу әдістерінің тиімділігі және тағы басқалары. Негізгі қауіпсіздік деңгейі (базалық қауіпсіздік) - ақпараттық жүйенің міндетті минималды деңгейі. Бірқатар елдерде бұл деңгейді анықтау критерийлері бар. Мысал ретінде осы елдің мемлекеттік институттары үшін ақпараттық қауіпсіздік саласындағы минималды талаптарды анықтайтын Ұлыбритания критерийлерін - CCTA базалық қауіпсіздік зерттеуін келтірейік. Германияда бұл өлшемдер BSI стандартында көрсетілген. NASA, X / Open, ISACA және басқалар үшін бірқатар ұйымдар бар. Біздің елде ИСО / МЭК 27001-2008, «Ақпараттық технологияларды енгізу бойынша нұсқаулыққа сәйкес тәуекелдерді талдау және бағалау жүргізілуі керек. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар». Тәуекелдерді бағалау кезінде ақпараттық қауіпсіздікке төнетін қатердің сандық және сапалық көрсеткіштерге әсерін ескеру қажет. Қабылданған шаралардың құны қауіп-қатерлерді іске асырудан туындауы мүмкін зияннан аспауы керек. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шаралар мен шаралар жеткілікті мөлшерде жүзеге асырылады, тәуекелдерді азайтады, ал қорғау шараларының тиімділігі мен тиімділігі үнемі бағаланады.

Қазақстан Республикасы Білім және ғылым министрлігінің ақпараттық қауіпсіздігінің тәуекелдерін бағалау әдістемесі пайдаланылатын ақпараттық қауіпсіздік жүйелерінің өзектілігі мен экономикалық орындылығын анықтауға, сондай-ақ ақпараттық қауіпсіздік үшін қабылданатын шаралардың саладағы нормативтік-техникалық құжаттардың талаптарына сәйкестігін анықтауға арналған. ақпараттық қауіпсіздік.

Ақпараттық тәуекелдерді талдау қауіптер мен осалдықтардың түрлерін түсіну, олардың пайда болуы мен дамуын болжау, қорғау жүйесін құру және іске асыру үшін қажетті инвестициялар үшін қажет.

Тәуекел дегеніміз - ақпараттың ашылуы, өзгертілуі, жоғалуы немесе қол жетімді еместігі нәтижесінде туындауы мүмкін ықтимал залал. Тәуекел екі факторға байланысты - ақпарат құны және өңделетін ақпараттық жүйенің қауіпсіздігі.

Тәуекелді анықтау негізінде тәуекелдерге талдау жасау үшін ақпараттық жүйе туралы келесі ақпарат қажет:

1. Оның маңыздылығын көрсететін құнды ақпарат тізімі;

2. Ақпараттық жүйенің осалдығы және оған әсер ететін қауіптер туралы ақпарат.

Тәуекелді талдау қадамдары:

Министрліктің ақпараттық қауіпсіздігінің қатерін бағалау алгоритмі (бұдан әрі - АЖ) бірнеше кезеңнен тұрады (№1 сурет):

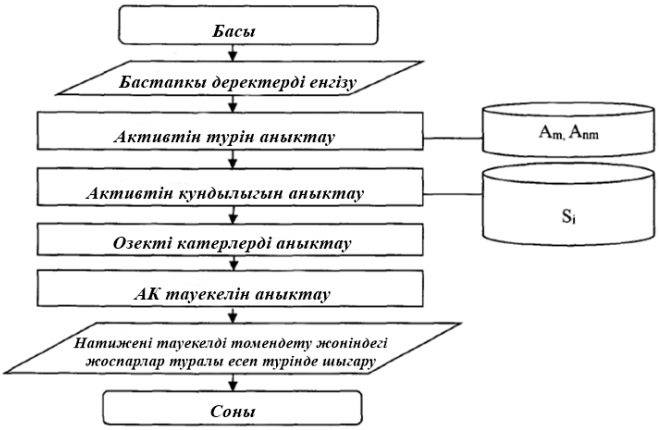
1. Актив түрін анықтау;

2. Активтердің құнын анықтау (Белгілеу - Si);

3. Қатерлерді және олардың сәйкес осал тұстарын анықтау, қауіптерді іске асыру мүмкіндігін бағалау (белгілеу - Vry);

4. Ақпараттық қауіпсіздік қауіп-қатерін анықтау (Анықтама - R);

5. Ақпараттық қауіпсіздікке қауіп төндіретін жоспарларды құру.



№1 сурет. Ақпараттық қауіпсіздік тәуекелін бағалау алгоритмінің диаграммасы

Тәуекелді талдаудың көптеген әдістері бар. Олардың кейбіреулері қарапайым қарапайым кесте әдістеріне негізделген және мамандандырылған бағдарламалық құралдарды қолдануды қарастырмайды, ал басқалары, керісінше, белсенді қолданады. Тәуекелдерді басқаруға деген қызығушылықтың артуына қарамастан, қазіргі уақытта қолданылып жүрген әдістер салыстырмалы түрде тиімсіз, өйткені көптеген компанияларда бұл процесс әр бөлімше дербес жүзеге асырылады. Олардың іс-әрекеттерін орталықтандырылған бақылау көбінесе жоқ, бұл бүкіл ұйымда тәуекелдерді басқарудың бірыңғай және тұтас тәсілін жүзеге асыру мүмкіндігін жоққа шығарады.

Ақпараттық қауіпсіздік тәуекелдерін бағалау мәселесін шешу үшін қазіргі кезде көбінесе келесі бағдарламалық қамтамасыз ету жүйелері қолданылады: CRAMM, FRAP, RiskWatch, Microsoft Security Assessation құралы (MSAT), GRIF, CORAS және басқалар. Барлық белгілі техникаларды бөлуге болады:

- тәуекелді бағалауды сапалы деңгейде қолданатын әдістер (мысалы, «жоғары», «орташа», «төмен» шкаласы бойынша), мұндай әдістер FRAP қамтиды;

- сандық әдістер (тәуекел сандық мәні бойынша бағаланады, мысалы, күтілетін жылдық шығындардың мөлшері), осы әдісі RiskWatch –қа жатады;

- аралас бағалауды қолданатын әдістер (бұл тәсіл CRAMM, MSAT әдіснамасында қолданылады).

АЖ тәуекелдерін басқарудың белгілі бір әдістемесін қолданар алдында оның компанияның қажеттіліктерін, оның көлемін ескеретініне, сонымен қатар халықаралық озық тәжірибелерге сәйкес келетініне және процестер мен талап етілетін іс-әрекеттердің толық сипаттамасына ие екендігіне көз жеткізу керек.

CRAMM

Бұл әдіс бизнес-процестердің сипаттамасы немесе тәуекелдерді бағалау туралы есептер сияқты растайтын құжаттаманы ескермейді. Тәуекелдерді басқару стратегиясына келетін болсақ, CRAMM оларды азайту үшін тек әдістерді қолдануды қарастырады. Айналып өту

немесе қабылдау сияқты тәуекелдерді басқарудың осындай тәсілдері қарастырылмайды. Басқару тәсілдерін интеграциялау процесі және қандай да бір тәсілдің мақсатын сипаттау әдістемеде жоқ.

CRAMM-ді іс жүзінде қолдану жоғары білікті мамандарды тарту қажеттілігімен; тәуекелдерді бағалау процесінің еңбек сыйымдылығы мен ұзақтығымен байланысты. Сонымен қатар, лицензияның жоғары құнын атап өткен жөн.

ГРИФ

ГРИФ әдістемесі бағалаудың сандық және сапалық әдістерін қолданады сондай-ақ компания қабылдауы мүмкін соңғы шарттарды айқындайды, қауіпсіздік шараларын енгізуге инвестицияларды қайтару есебін қамтиды. Тәуекелдерді талдаудың басқа әдістемелерінен айырмашылығы, ГРИФ тәуекелдерді төмендетудің барлық тәсілдерін ұсынады (айналып өту, төмендету және қабылдау). Осы әдістеме бизнес-үдерістерді сипаттау немесе АҚ тәуекелдерін жүргізілген бағалау бойынша есептер сияқты құжаттаманы ескереді.

RiskWatch

Бұл әдістеме тәуекелдерді бағалаудың сандық және сапалық тәсілдерін қолданады. Осы әдісті пайдалана отырып, тәуекелдерді талдау жөніндегі жұмыстардың еңбек сыйымдылығы салыстырмалы түрде аз емес. Мұндай әдіс, егер ұйымдық және әкімшілік факторларды есепке алмай, қорғаудың бағдарламалық-техникалық деңгейінде тәуекелдерге талдау жүргізу талап етілсе қолайлы. RiskWatch маңызды артықшылығы интуитивті түсінікті интерфейс және жаңа санаттарды, сипаттамаларды, мәселелерді және т. б. енгізу мүмкіндігімен қамтамасыз етілетін әдістің үлкен икемділігі болып табылады.

Қаралған әдістемелер "тәуекелдер" және "процестер (тәуекел элементтерін пайдалану)" топтарының талаптарына жақсы сәйкес келеді, бірақ олардың кейбіреулері (CRAMM) "Мониторинг" және "басқару" бөлімдеріне, сондай-ақ "процестер"көптеген кіші бөлімдеріне сәйкес кемшіліктерге ие. Бірнешелері (ГРИФ, RISKWATCH) тәуекелдерді қайта бағалауды өткізу кестесін жасау жөнінде толық ұсыныстар береді.

Қолданылған әдебиеттер тізімі

1. Баранова Е.К., Бабаш А.В. Ақпараттық қауіпсіздік және ақпаратты қорғау. -М.:INFRA-M_RIOR, 2014 жыл.
2. В.М. Нечунаев. Оценка рисков информационной безопасности
3. Махмутов А. «Сыртқы саясаттың болашағы және Қазақстанның халықаралық стратегиясының жаңа тұжырымдамалары» Қазақстан Республикасының Тұңғыш Президенті - Елбасы Қоры жанындағы Әлемдік экономика және саясат институты. - 2012 .- 12 наурыз.
4. ISO/IEC 17799. Information Technology-Code of practic for information security management.2000.
5. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. –М.: ИНФРА-М_РИОР, 2014.

ОӘЖ 681.5.01

ӘЛЕУМЕТТІК ОБЪЕКТІЛЕРГЕ ЖЫЛУ БЕРУ ҮДЕРІСІН АЛДЫН АЛА БАСҚАРУ ЖҮЙЕСІНІҢ СИНТЕЗІ

Жолдасқалиева Аида Шаменқызы

zholdaskalieva97@mail.ru

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің магистранты, Нұр-Сұлтан, Қазақстан

Ғылыми жетекшісі – Б.Р.Касимова

Аңдатпа. Ғимараттың жылуын алдын ала басқарудың біріктірілген жүйесі синтезделген. Басқару жүйесінің динамикалық компенсаторының синтезі және ғимаратқа жылу беру үдерісін алдын ала басқару жүйесінің параметрлік синтезі сипатталған.