РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

ӘОЖ 004.056.53

ЗАМАНАУИ БИЗНЕСТЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ҚАУІП-ҚАТЕРЛЕРІН БАҒАЛАУ КЕЗЕҢДЕРІ

Адамжанов Тлек Болатханұлы
tlek86@mail.ru
Л.Н.Гумилев атындағы ЕҰУ «6М060200-Информатика» мамандығының 2 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.Сексенбаева

Ақпараттық қауіпсіздіктің (әрі қарай – АҚ) қауіп-қатерлерін басқару – заманауи бизнестің негізгі міндеттерінің бірі болып табылады. Оның басты мақсаты маңызды деректерді нақты қатерлерден қорғау. Алайда, бұл мәселедегі көптеген сұрақтар компанияның басшылығына, оның АҚ мәселелерін терең түсінуі мен біліктілігіне байланысты болады. Қазіргі заманда бизнестің дамуына тікелей немесе жанама әсер ететін мыңдаған ақпараттық қатерлер бар. Сол қатерлерді алдына алу үшін компания қажетті қорғаныс шараларын іске асыруы қажет. Жалпы ақпараттық ресурстардың қорғалу деңгейі мен потенциалды қатерлерден қорғануға бағытталған шаралардың деңгейі компанияның COBIT және басқа да стандарттарда көрсетілген кемелдік деңгейіне байланысты болады.

АҚ қауіп-қатерлерін басқару мекемедегі АҚ басқару жүйесінің (әрі қарай – АҚБЖ) фундаменті болып табылады. АҚ қауіп-қатерлерін басқару АҚБЖ құрамына кіретін ішкі жүйелердің ең бастысы және маңыздысы болып табылады. АҚБЖ басқару мен қажетті ресурстарды бөлу бойынша стратегиялық шешімдер қауіп-қатерлерді бағалау арқылы анықталады.

Қауіп-қатерлерді бағалау мекеменің АҚ-ін басқаратын тиімді механизмі бола отырып, келесі мәселелерді жүзеге асырады:

- компанияның ақпараттық жүйелерін анықтайды, әрі бағалайды;
- ақпаратты қорғау құралдарын еңгізудің қажеттілігін бағалайды;
- еңгізілген ақпаратты қорғау құралдарының тиімділігін бағалайды.

АҚ бойынша заманауи әдебиттерде қауіп-қатерлерді бағалау процесін басты екі кезеңге бөліп қарастырады: қауіп-қатерлерді талдау және қауіп-қатерлерді бағалау.

Қауіп-қатерлерді талдау өз ішіне активтерді анықтау, бизнес пен заңның талаптарын анықтау, активтердің құндылығын анықтау және қатерлер мен осалдылықтарды анализдеу сияқты процесстерді қамтиды. Ал қауіп-қатерлерді бағалау қауіп-қатерлердің сапалық және сандық мөлшерін анықтау мен қауіп-қатерлерді саралаудан тұрады.

Ендігі кезекте, жоғарыда аталған қауіп-қатерлерді бағалаудың әрбір кезеңі жеке-жеке сипатталатын болады. Ең алдымен активтерді анықтауға баса көңіл бөлу қажет, себебі бұл кезеңде компанияның қатерге ұшырауы мүмкін болған барлық бағалы активтері анықталады. Әсіресе ақпараттық активтерге баса назар аударылады, сонымен бірге олармен өзара байланысты ресурстар да қарастырылады. А. Астаховтың «Искусство управления информационными рисками» атты кітабында активтерді анықтау барысында жүзеге асырылуы қажет іс-шаралардың тізімі келтіріледі:

- бизнес-процесстердің моделін құрастыру;
- активтерді инвентаризациялау;
- активтердің тізімін құру;
- активтер тізімі арасындағы байланысты анықтау;
- активтердің моделін құру;
- активтердің иелерін және олардың міндеттерін анықтау;
- активтердің қауіпсіздігін қаматмасыз ету үшін міндеттерді бөлу;
- активтерді классификациялау и категорияларға бөлу;
- активтерді қолдану ережелерін анықтау.

Ақпараттық қауіп-қатерлерді басқару процесі барысында көптеген компаниялар заңды және нормативті талаптармен бетпе-бет кезігетіні жасырын емес. Мұндай заңды нормалар мекемелермен ақпаратты (жеке, қаржылық және операциялық) басқаруға және аудит жасауға арналған тиімді механизмдерді еңгізу үшін қажет. Көптеген заңды және нормативті актілер қауіп-қатрелерді бағалауды осы басқарудың тиімді механизмдерінің маңызды элементі ретінде қарастырады.

Қазақстан Республикасының осы салаға, яғни ақпараттық қауіпсіздікке қатысты заңдары әртүрлі деңгейдегі нормативті-құқықтық актілер ретінде ұсынылған. Олар Қазақстан Республикасының Конституциясы, Азаматтық, Қылмыстық және Әкімшілік кодекстардан бастап мамандандырылған, фундаменталды көздер ретінде қарастырылатын «Ақпараттандыру туралы», «Қазақстан Республикасының ұлттық қауіпсіздігі туралы», «Дербес деректер және оларды қорғау туралы» заңдарына дейін атап өтуге болады.

Айта кетерлік, «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысында ақпараттық-коммуникациялық технологиялар (әрі қарай – АКТ) саласындағы қауіп-қатерлерді басқару кезеңдері келесі түрде келтірілген:

«МО-да немесе ЖАО-да АКТ саласындағы тәуекелдерді басқару мақсатында:

1) ҚР СТ 31010-2010 «Тәуекел менеджменті. Тәуекелді бағалау әдістері» Қазақстан Республикасы стандартының ұсынымдарына сәйкес тәуекелдерді бағалау әдісін таңдау және тәуекелдерді талдау рәсімдерін әзірлеу;

2) сәйкестендірілген және сыныпталған активтердің тізбесіне қатысты тәуекелдерді сәйкестендіру жүзеге асырылады, ол мыналарды қамтиды:

– АҚ қатерлерін және олардың көздерін айқындау;
– қатерлердің іске асырылуына әкеп соғуы мүмкін осалдықтарды айқындау;
– ақпараттың таралу арналарын анықтау;
– бұзушы моделін қалыптастыру;

3) сәйкестендірілген тәуекелдерді қабылдау өлшемшарттарын таңдау;

4) мыналарды:

– ҚР СТ 13335-2008 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық және коммуникациялық технологияларды қорғауды басқару" Қазақстан Республикасы стандартының талаптарына сәйкес сәйкестендірілген тәуекелдердің тәуекелдерін бағалауды (қайта бағалауды);

– ықтимал нұқсанды айқындауды қамтитын АҚ қатерлері (тәуекелдері) каталогын қалыптастыру;

5) АҚ қатерлерін (тәуекелдерін) бейтараптандыру немесе төмендету жөніндегі іс-шараларды қамтитын оларды өңдеу жоспарын әзірлеу және бекіту жүзеге асырылады.»

Осы аталған нормативті-құқықтық актілерден Қазақстан Республикасының ақпараттық қауіпсіздікке, оның ішінде қауіп-қатерлерді бағалауға қаншалықты мән беріп, үнемі қолдау көрсетіп отыратынын көруге болады.

Сонымен, қауіп-қатерлерді бағалаудың келесі кезеңі активтердің құндылығын анықтау болып табылады. Компанияның активтерін бағалау деп компания активтерінің моральдық және физикалық тозуын ескере отырып, қалыпқа келтіру бағасын есептеуге негізделген нарықтық немесе басқа да бағасын анықтау процедурасын атайды. Активтерді қорғаудың қажетті деңгейін анықтау үшін осы активтердің бизнестегі маңыздылығын ескере отырып бағалау қажет.

Жоғарыда атап өткен А. Астаховтың «Искусство управления информационными рисками» атты кітабында активтердің құндылығын анықтау кезеңдері келтіріледі:

– активтер құндылығының шкаласын анықтау;
– нұқсанды бағалау өлшемдерін анықтау;

– бағалау үшін активтердің иелері мен пайдаланушыларынан бастапқы деректерді алу;

– активтің құпиялылығын, тұтастығын және қолжетімділігін бұзу нәтижесінде бизнеске тигізетін әсерін анықтау;

– әрбір үш қасиет үшін жеке-жеке активтің құндылығын анықтау.

Жоғарыда аталып өткен активтер мекемеге төндіретін қатерлердің басты объектілері болып табылады. Осы орайда, қауіп-қатерлерді бағалаудың келесі кезеңі қатерлер мен осалдылықтарды сәйкестендіруге өтеміз.

Жалпы Қазақстан Республикасының Киберқауіпсіздік тұжырымдамасында АҚ қатеріне келесідей анықтама берілген: «Ақпараттық қауіпсіздік қауіп-қатері – әбден болуы мүмкін оқиға, процесс немесе құбылыс, ол ақпаратқа немесе ақпараттық жүйенің немесе ресурстың компоненттеріне әсер ету арқылы иеленушілер мен пайдаланушылардың мүдделеріне тікелей немесе жанама зиян келтіруге әкеліп соқтыруы мүмкін.» Қатер нәтижесінде компанияға нұқсан келтірілетін жағымсыз оқиғаларға себеп болуы мүмкін.

Бұл нұқсан компанияның иелігіндегі ақпаратқа шабуыл жасау нәтижесінде болуы мүмкін және оны заңсыз айғақтауға, өзгертуге, бұзуға, жоюға, қолжетіспеушіліке және жоғалтуға алып келуі мүмкін. Қатерлер кездейсоқ немесе әдейі көздерден немесе оқиғалардан келуі мүмкін. Қатерлерді іске асыру барысында жүйелердің, қосымшалардың немесе сервистердің бір немесе бірнеше осалдылықтары қолданылады. Қатерлер мекеменің ішінен де, сырттан да төнуі мүмкін.

АҚ қатерлері әртүрлі. Бұл қатерлердің тізімі BS 7799-3 и ISO 27005 стандарттарының қосымшаларында келтірілген. АҚ-ің мың қатеріне нақты сипаттамаларының бірі немістің ашық BSI IT Baseline Protection Manual (АТ қорғау бойынша бастапқы нұсқаулық) атты стандартында кездестіруге болады.

Әрбір сәйкестендірілген қатер үшін осалдылықтар тізімі анықталады. Осы осалдылықтар арқылы қатерді іске асыру мүмкін болады. Сондай-ақ, мекемедегі қауіпсіздік пен ақпараттық жүйелердің қорғалғандығын бақылайтын аудит нәтижелері, адами факторлардың әсері және де қолданыстағы бақылау механизмдерінің (ұйымдастырушылық және техникалық) әлсіз немесе тіптен жоқ болу фактілері есепке алынады.

Қауіп-қатерлерді бағалау бойынша іс-шараларының алдында немесе қатерлер мен осалдылықтарды сәйкестендірудің алдында қолданыстағы қауіпсіздік механизмдері сәйкестендірілуі қажет. Бұл қатерлер мен осалдылықтарды шынайы бағалауға және оларды толық сәйкестендіру үшін қажет болады. Сонымен қатар, қауіп-қатерлерді өңдеу нұсқалары мен қауіп-қатерлерді басқару бойынша іс-шараларды қарастырған кезде де керек.

Қауіп-қатерлерді бағалаудың келесі кезеңі олардың сандық және сапалық мөлшерлерін анықтау болып табылады. Сонымен, егер зерттеліп отырған қатерлерді, және де олармен байланысты қауіп-қатерлерді ақша, пайыз, уақыт, адам ресурстары және т.б. сияқты соңғы сандық мәндермен салыстыруға келсе, онда қауіп-қатерлердің сандық бағалау әдісі қолданылады. Егер ақпараттық қауіпсіздік қатерлері іске асырылатын болса, онда бұл әдіс қауіп-қатерін бағалайтын объектілердің нақты мәнін алуға мүмкіндік береді.

Сандық әдіс кезінде қауіп-қатерлерін бағалайтын барлық элекменттерге нақты және шынайы сандық мән беріледі. Бұл мәндерді алу алгоритмі көрнекті, әрі түсінікті болу керек. Бағалау объектісі ретінде ақша түріндегі активтің құндылығы, қатерлерді іске асыру ықтималдылығы, қатерлерді іске асрыудың кесірінен туындаған нұқсан, қорғаныс шараларының бағасы және т.б. болуы мүмкін.

Сапалық әдіс барысында бағалау объектісі үшін сандық немесе ақшалай өлшемдер қолданылмайды. Оның орынына бағалау объектісіне үш балды (төмен, орташа, жоғары), бес немесе сегіз балды (0....8) шкала бойынша сарланған көрсеткіштер қолданылады. Қауіп-қатерлерді сапалық әдіс бойынша бағалау барысында мәліметтерді жинау үшін мақсатты топтардан сұрау, сұхбатасу, сауалнама, жеке кездесулер қолданылады.

Ақпараттық қауіпсіздіктің қауіп-қатерлерін сапалық әдіс арқылы талдау, қатерлер қарастырылып отырған саладағы тәжірибелі, әрі құзыретті қызметкерлерді тарту арқылы жүзеге асырылуы қажет.

Қауіп-қатерлердің мөлшерін анықтағаннан соң, оларды өңдеу басымдылығын анықтау мақсатында бұл қауіп-қатерлерді саралу қажет. Келесі кесте (Кесте 1) нұқсан факторлары (актив құндылығы) мен оқиға ықтималдылығын (қатер мен осалдылық қосылып, нақты бір оқиғаның себебі болады) байланыстыру үшін қолданылуы мүмкін. Ең бірінші, мысалы әрбір актив бойынша 1-ден 5-ке дейін, нұқсан бағаланады (b бағаны). Екінші, оқиғаны іске асыру ықтималдылығы бағаланады, мысалы әрбір оқиға бойынша 1-ден 5-ке дейін (c бағаны). Келесі сатыда b мен c-ны көбейту арқылы қауіп-қатер мөлшері есептелінеді. Және ең соңында оқиғалар маңыздылығы бойынша саралануы мүмкін. Айта кету керек, бұл мысалда 1 дегеніміз ең төмен нұқсан және ең төмен ықтималдылық.

Кесте 1

Қауіп-қатер мөлшері бойынша оқиғаларды саралайтын матрица

Оқиға дескрипторы (a)	Нұқсан (ресурс бағасы) (b)	Іске асыру ықтималдылығы (c)	Қауіп-қатер мөлшері (d)	Оқиға категориясы (e)
Оқиға A	5	2	10	2
Оқиға B	2	4	8	3
Оқиға C	3	5	15	1
Оқиға D	1	3	3	5
Оқиға E	4	1	4	4
Оқиға F	2	4	8	3

Сонымен, тоқсан ауыз сөздің тобықтай түйіні, кез-келген заманауи компаниядағы АҚ-тің қауіп-қатерлерін бағалау жоғарыда сипатталып өткен кезеңдерден тұрады және ол кезеңдер әрбір активтің түріне орындалуы керек. АҚ қауіп-қатерінің алынған мәні қауіп-қатер деңгейін төмендету бойынша ұсыныстар жасау үшін және компанияның АҚ-ін қамтамасыз ету бойынша тиімді шараларды қабылдау үшін қажет. Егер қауіп-қатердің қорытынды мәні шамамен 5 пайыздан төмен болса, онда компанияда АҚ талаптары орындалғаны жайлы, әрі активке қатысты қауіп-қатердің мәні ұйғарынды екендігі туралы қорытынды жасауға болады. Алайда, АҚ қауіп-қатерлерін әрдайым бағалап тұру қажет. Ал егер қауіп-қатердің қорытынды мәні 5 пайыздан жоғары болса, онда компанияда АҚ талаптары орындалмай жатқандығы жайлы және активке қатысты қауіп-қатер деңгейі жоғары және жедел түрде қажетті шешім қабылдау керектігі жайлы тұжырымдауға болады.

Қолданылған әдебиеттер тізімі

1. Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы.

2. Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.

3. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010, 312 с.

4. Международный стандарт ISO/IEC 27005:2011. Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности BS ISO/IEC 27005:2011.

5. https://kontur.ru/articles/1691