ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ЖӘНЕ БАСҚАРУ

Информационная технология
ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ

ҚР СТ 34.029 - 2008

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ЖӘНЕ БАСҚАРУ

ҚР СТ 34.029 - 2008

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасы Ақпараттандыру және байланыс жөніндегі агенттігі **ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігі Техникалық реттеу және метрология комитетінің 2008 жылғы 25 ақпандағы № 107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жылы
ТЕКСЕРУДІҢ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Жалпы ережелер

Осы құжат мыналарға: қатысатындарға пайдалы болады.

– Ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) әзірлеу мен сүйемелдеуге;

– АҚБЖ-ны сертификаттауды дайындауға,

– ұйымның АҚБЖ аудитына (бірінші тараптың аудиті – ішкі аудит сияқтылар, екінші тараптың аудиті, мысалы сертификаттаудың тәуелсіз органдары орындайтын аудиттер).

Ұйым тәуекелдерді бағалау жөніндегі іс-қимылдардың нәтижесін түсіндіру мен негіздеме үшін, әсіресе сертификациялау процесінің маңызды бөлігі ретіне пайдаланатыны маңызды, А қосымшасынан неге басқарудың нақты мақсаттары мен басқарудың құралдары таңдап алынды, неге олардың кейбіреу таңдап алынбады және неге (қажет кезінде) *ҚРСТ ИСО/МЭК 27001* стандартында санамаланғандарға қосымша басқару құралдары таңдап алынды.

АҚБЖ ұғымы

Ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) бизнес-тәуекелдерді бағалауға негізделген және ақпараттық қауіпсіздікті әзірлеу, іске асыру, пайдалану, мониторинг, ілесу мен жетілдіру үшін арналған басқарудың жалпы жүйесінің бір бөлігін білдіреді. Басқару жүйесі ұйымдастырушылық құрылымды, саясатты, жоспарларды әзірлеуді, жауапкершіліктерді бөлу, нұсқаулықты, рәсімдерді, процестер мен ресурстарды қамтиды. АҚБЖ-ны пайдалану саласы ақпараттарды өңдеу, сақтау және беру үшін пайдаланылатын маңызды ресурстарды, жүйелерді, қосымшаларды, сервистерді, желілер мен технологиялардың қамти отырып, ұйымдардың толық немесе бір бөлігі сияқты ұйымдардың терминдерінде айқындалуы мүмкін. Бұл ретте ақпараттың өзі ресурс ретінде қаралады. Осы стандартта осы тәрізді ақпаратпен байланысты элементтердің жиынтығы «ақпараттық жүйе» немесе «ақпараттық жүйелер» деп аталады. Мұндай контексте АҚБЖ мыналарды:

– ұйымның барлық ақпараттық жүйелері;

– ұйымның кейбір ақпараттық жүйелері;

– жеке ақпараттық жүйені қамтуы мүмкін.

Ұйым анықтайтын АҚБЖ-ны қолдану саласы, осы бөлімнің соңындағы кестеде көрсетілгендей, сертификаттаудың мәні болып табылады. Ұйымға өз бизнесінің әр түрлі бөлімшелері немесе аспектілері үшін әр түрлі АҚБЖ-ны белгілеу талап етілуі мүмкін. Мысалы, басқа компаниялармен нақты сауда қатынастары үшін АҚБЖ-ны белгілеу мүмкін. Бір немесе бірнеше әртүрлі АҚБЖ көмегімен жүзеге асырылуы мүмкін іскерлік серіктестерді қажетті жіктеулермен қамтамсыз ету үшін ұйымның өзінің

бизнесін құрылымдауы тағы бір мысал бола алады. Бір немесе бірнеше әртүрлі АҚБЖ-мен қамтылатын әртүрлі сценарийлер болуы мүмкін.

ЖІБТ моделі

«Жоспарлау – Іске асыру – Бағалау – Түзету (Plan-Do-Check-Act)» (Модель ЖІБТ (PDCA)) ретінде белгілі модел *ҚРСТ ИСО/МЭК 27001* стандартында пайдаланылады. Осы модел АҚБЖ-ны әзірлеу, іске асыру, мониторинг, талдау, сүйемелдеу және жетілдіру үшін негіз ретінде пайдаланылады. Осы модел туралы барынша егжей-тегжейлі ақпарат *ҚРСТ ИСО/МЭК 27001* және *СТ РК* стандарттарында келтірілген.

Осы стандарттың құрылымы

Осы стандарт екі бөлімнен тұрады:

– Бірінші бөлікте:

– Ақпараттық қауіпсіздік дегеніміз не?

– Неге қорғау шараларын қабылдау қажет,

– Қажетті шараға қалай қол жеткізуге болатындығы туралы жалпы мәліметтер мазмұндалады.

– Екінші бөлікте:

– Тәуекелдерді бағалаудың компоненттері мен олардың арасындағы байланысты сипаттау,

– Тәуекелдерді бағалау процесіне қосылатынды егжей-тегжейлі сипаттау,

– Тәуекелдерді бағалау үшін ұйымдастыруда іске асырылуы мүмкін жалпы тәсілдің немесе стратегияның әр түрлі нұсқаларын сипаттау келтіріледі.

Бұған қоса стандарт ҚР СТ ИСО/МЭК 17799 және *ҚР СТ ИСО/МЭК 27001* стандарттарына қосылған басқарудың мақсаттары мен құралдарына қатынасы бойынша қауіптер мен күдіктіліктің барынша егжей-тегжейлі мысалдары келтірілген бірнеше қосымшалардан, сондай-ақ тәуекелдерді бағалау мен тәуекелдерді өңдеу үшін пайдаланылатын әдістер мен инструменталдық құралдар туралы ақпараттан тұрады.

***ҚР СТ ИСО/МЭК* 17799 стандартын қолданылу саласы мен мақсаты**

ҚР СТ ИСО/МЭК 17799:2005 стандарты ақпараттық қауіпсіздікті басқарудың нақты қолдану жөніндегі нұсқауды ұсынады. Стандарттың басты мақсаттары мыналарды:

– Қауіпсіздікті әзірлеуші, іске асырушы және бағалаушы басқаруды тәжірибеде ұйымдастыру үшін жалпы негіз;

– Ұйымдардың арасындағы іскерлік қатынастардың құпиялылығын қамтамасыз етуден тұрады.

ҚР СТ ИСО/МЭК 17799 стандартында басқару мақсатының жиынтықтығы, сондай-ақ басқару мақсаттарын қолдау үшін іске асырылуы

мүмкін қауіпсіздікті басқару құралдарының толық жиынтығы айқындалады. Басқарудың бұл құралдары осы сәтте Ұлыбританияда да, халықаралық ауқымда да коммерциялық, өнеркәсіптік және мемлекеттік ұйымдарда іске асырылатын ақпараттық қауіпсіздіктің басқару құралдарына негізделген.

Басқарудың бұл құралдары қоршаған ортамен немесе пайдаланылатын технологиялармен байланысты шектеулер сияқты шектейтін факторларды ескере отырып, ақпараттық қауіпсіздікті нақты қамтамасыз ету үшін ұсынылады. Басқарудың кейбір құралдары әрбір бизнес-ортада қолданылмауы мүмкін, және оларды жергілікті жағдайға қатысты сайланбалы пайдаланған жөн.

***ҚР СТ ИСО/МЭК* 27001 стандартының қолданылу саласы мен мақсаты**

ҚР СТ ИСО/МЭК 27001 стандарты ұйымның жалпы бизнес-тәуекелдерінің контекстінде құжаттамаланған АҚБЖ әзірлеуге, іске асыруға, пайдалануға, бақылауға, талдауға, сүйемелдеуге және жетілдіруге талаптарды белгілейді. Осы стандартта жекелеген ұйымдар мен олардың бөліктерінің қажеттіліктеріне сүйенген қауіпсіздікті басқару құралдарын іске асыруға талаптар белгіленеді.

АҚБЖ ақпараттық ресурстарды қорғайтын және мүдделі тараптар үшін құпиялылықты қамтамасыз ететін қауіпсіздікті басқарудың баламалы және тең мөлшерлі құралдарды қамтамасыз ету үшін әзірленеді. Бұл өз кезегінде бәсекеге қабілеттілікті, ақша қаражаттарының ағынын, рентабелділікті, құқықтық талаптар мен коммерциялық саясатқа сәйкестікті ұстап тұруға және арттыруға мүмкіндік береді.

Тәуекелдерді бағалау және *ҚР СТ ИСО/МЭК 27001* стандартының контекстінде басқару құралдарын таңдау

Ұйым әзірленетін және сүйемелдейтін АҚБЖ-ны қолдану саласына қосылған, ақпараттық жүйелер үшін тәуекелдерге тартылған ақпараттар мен басқа ресурстардың коммерциялық құндылықтарын ескере отырып, қауіпсіздіктерді бұзумен байланысты тәуекелдерді бағалауды орындау қажет. Ұйым таңдап алынған және АҚБЖ-ға құжаттандырылған басқару мақсаттары мен басқару құралдары бизнестің нақты жағдайлары мен шарттарына сәйкес тәуекелдерді бағалау процесінің көмегімен қауіпсіздікті бұзу тәуекелдерін ұқсастыру мен бағалау процесінің нәтижесінде белгіленген болуы тиіс. (сондай-ақ 3.1 - 3.5 бөлімін қараңыз).

Тәуекелдерді бағалау нәтижелерінің негізінде АҚБЖ қамтылған ұйымдардың ресурстарын теңестірілген тәуекелдерден қорғауға мүмкіндік беретін *ҚР СТ ИСО/МЭК 27001* стандартының А-қосымшасынан басқарудың қажетті құралдарын таңдауға болады. АҚБЖ-ның сертификациялау үшін ұйым теңестірілген тәуекелдерге ақпараттық қауіпсіздікті қамтамасыз ету үшін таңдап алынған басқару мақсаттары мен басқару құралдарының барабар екендігін көрсетуге қабілетті болуы тиіс.

ҚР СТ ИСО/МЭК 27001 **стандартына енгізілмеген басқару құралдары**

Басқару мақсаттары мен басқару құралдарын таңдап алу процесі *ҚР СТ ИСО/МЭК 27001* стандартының А-қосымшасында келтірілмеген басқару құралдарын теңестіру мен іске асыруды жоққа шығармайды. Бағаланған тәуекелдер үшін стандартта келтірілгеннен өзгеше басқару құралдарын қолдану қажет етілетін жағдай да болуы мүмкін. Басқарудың бұл құралдары басқару құралдарының басқа да каталогтарынан, кітапханалардан, стандарттар мен өзге де көздерден таңдап алынуы мүмкін. Сертификаттау үшін стандартта келтірілмеген басқару құралдарын қолданудың негіздемесі *ҚР СТ ИСО/МЭК 27001* стандартынан таңдап алынған басқару құралдары үшін де осылайша құжаттандырылған болуы тиіс.

«Жоспарлау – Іске асыру – Бағалау – Түзету (Plan-Do-Check-Act)» процесін егжей-тегжейлі сипаттау

ҚР СТ ИСО/МЭК 27001 стандартында құжаттандырылған АҚБЖ-ны әзірлеу мен басқару сипатталады. *С*тандартқа сәйкес сертификациялау немесе қайта сертификаттауды алуға ұмтылған ұйым АҚБЖ процесіне төмендегі кестеде сипатталғандай (барынша егжей-тегжейлі ақпарат осы құжаттың 3-бөлімінде келтірілген) Жоспарлау – Іске асыру – Бағалау – Түзету моделін қолдануы тиіс:

Тақырып/Тапсырма	**Ұйымның міндеттері**
АҚБЖ-ны әзірлеу (4.2.1-бөлім)	а) АҚБЖ-ны қолдану саласын белгілеу; б) АҚБЖ саясатын белгілеу; в) тәуекелдерді бағалауға жүйелік тәсілді белгілеу; г) тәуекелдерді теңестіру; д) тәуекелдерді бағалау; е) тәуекелдерді өңдеу нұсқаларын теңестіру мен бағалау; ж) басқару мақсаттары мен басқару құралдарын таңдау; з) қолданушылық туралы ережені дайындау; и) басшылықтан бекітуді алу.
АҚБЖ-ны іске асыру және пайдалану (4.2.2-бөлімі)	а) тәуекелдерді өңдеу жоспарының ережелерін қалыптастыру; б) тәуекелдерді өңдеу жоспарын іске асыру; в) барлық таңдап алынған басқару мақсаттары мен басқару құралдарын іске асыру; г) оқыту мен хабарлау бағдарламаларын іске асыру; д) АҚБЖ-ны пайдалануды қолдану; е) АҚБЖ үшін ресурстарды басқару.
АҚБЖ-ны мониторингі және талдау (4.2.3-бөлімі)	а) мониторинг рәсімдерін орындау; б) АҚБЖ тиімділігін тұрақты талдауды жүзеге асыру; в) қалдық тәуекелдердің деңгейі мен тәуекелдердің теңестірілген ыңғайлы деңгейлеріне талдау жүргізу; г) АҚБЖ-ның ішкі аудитін жүргізу; д) басқару персоналдарына АҚБЖ талдауын тұрақты жүргізу; е) АҚБЖ-ның тиімділігіне әсер етуі мүмкін барлық оқиғаларды тіркеу.

АҚБЖ-ны сүйемелдеу және жетілдіру (4.2.4-бөлімі)	а) теңестірілген жетілдіруді іске асыру; б) түзейтін және тікелей жариялайтын тиісті шараларды қабылдау; в) барлық мүдделі тараптарға нәтижелер туралы хабарлау; г) жетілдірудің қойылған мақсаттарға қол жеткізетініне көз жеткізу.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ТӘУЕКЕЛДЕРДІ БАҒАЛАУ МЕН БАСҚАРУ

Енгізілген күні 2008.07.01.

1 Қолданылу саласы

Осы стандартта *ҚР СТ ИСО/МЭК 17799* және *ҚР СТ ИСО/МЭК 27001* стандарттарының контекстінде тәуекелдерді бағалау мәселесі қаралады.

Осы стандарттың негізгі мақсаты – тәуекелдерді бағалау процесінің және тәуекелдерді бағалау кезінде орындалатын барлық рәсімдердің негізінде жатқан пайдаланылатын терминдер мен негізгі ұғымдар туралы жалпы ұсыным беру.

Осы стандарт мынадай:

– *ҚР СТ ИСО/МЭК 17799* және *ҚР СТ ИСО/МЭК 27001* стандарттарының контекстінде тәуекелдерді бағалау процесін түсінуді қажетсінетін;

– өзінің ақпараттық қауіпсіздік басқару жүйесін әзірлейтін және сүйемелдейтін;

– өзінің ақпараттық қауіпсіздік басқару жүйесін сертификациялауға немесе қайталама сертификаттауға дайындалатын ұйымдарға арналған.

Ол сондай-ақ сертификаттауды жүргізуге қатысатын, тәуекелдерді бағалау процесін түсінуі қажет ұйымдар пайдалануға арналған.

Ақпараттық технологияны қауіпсіздікпен басқару жөніндегі нұсқаулықты пайдалану (Guidelines for the Management of IT Security) (GMITS)

«Ақпараттық технологияны қауіпсіздікпен басқару жөніндегі нұсқаулықты» (GMITS) – бұл ISO/IEC әзірлеген және АТ қауіпсіздікпен басқару жөніндегі нұсқаулықты халықаралық ауқымда танылған, осы стандарттың әр түрлі орындарында пайдаланылатын ақпараттар. GMITS көптеген алдыңғы қатарлы халықаралық компаниялар мен ұйымдар әзірлеген және келісілген қауіпсіздікті басқарудың нұсқаулары мен әдістерінің жиынтықтығын белгілейді.

GMITS осы стандартта баяндалған тәуекелдерді бағалау мен өңдеу процестері үшін ұғымдардың көпшілігі, тұжырымдар мен әдістер үшін базис қалыптастырады. Десе де GMITS стандартының атауында АТ қауіпсіздігі туралы айтылады, оның қолдану аясы осы шеңберден шығып кетеді, сондықтан осы нұсқаулықтардағы аталған қағидаттар ақпараттық қауіпсіздігіне де қолданылуы мүмкін.

Ресми басылым

Осы стандарттың 5 және 6 бөлігінде GMITS әр түрлі бөлімдерінде келтірілген ұсынымдар мен нұсқаулықтар қалайша *ИСО/МЭК 27001* стандарты бойынша сертификаттау процесімен үйлесімде ИСО/МЭК 17799 және *ИСО/МЭК 27001* стандарттарын жалпы қолданған жағдайда тәуекелдерді бағалау мен өңдеу процестерін қолдау үшін қолданылуы мүмкін екені түсіндіріледі.

Төменде GMITS ([1] - [5] қараңыз) стандартының бес түрлі бөлігіне шолу беріледі.

Ескертпе – Осы стандартта ескерілген ең соңғы басылымдар мен құжаттардың қолданыстағы редакциясын қолдану қажет.

GMITS. 1-бөлім. АТ қауіпсіздігі үшін тұжырымдамалар мен моделдер

GMITS стандартының 1-бөлігінде тәуекелдерді бағалау процесінде назарға алынуы тиіс негізгі қағидаттар мен моделдер сипатталады. Осы қағидаттарға шолу 5-бөлімде келтірілген. Мұндай қағидаттармен таныс емес осы стандартты пайдаланушы барынша толық ақпарат үшін GMITS стандартының, 1-бөлігінде жүгінуі тиіс.

GMITS. 2-бөлім. АТ қауіпсіздігін басқару мен жоспарлау

GMITS стандартының 2-бөлігінде ұйымдағы АТ қауіпсіздігін басқарумен байланысты әр түрлі әрекеттер сипатталады. Бұл бөлік АТ қауіпсіздігі процесінде басқару стратегиясын таңдаған және АТ қауіпсіздігі процесінде жауаптыларды тағайындаған кезде пайдаланылуы мүмкін. (бұл не қызықты ма? – ауд. ескертпелері). Бұған қоса оның ішінде басшылықтың көзқарасынан алғанда қауіпсіздік саясатын жоспарлаудың, әзірлеудің, түрлі кезеңдері, тәуекелдерді бағалау, АТ қауіпсіздігін басқару мен сүйемелдеудің құралдарын іске асыру сипатталады. GMITS стандартының 1-бөлігіндегі жағдайдағы сияқты осы стандартты пайдаланушылар барынша егжей-тегжейлі ақпарат үшін 2-бөлімге сүйенген жөн.

GMITS. 3-бөлім. АТ қауіпсіздігі үшін басқару әдістері

GMITS стандартының 3-бөлігінде АТ қауіпсіздігін табысты басқару үшін пайдаланылған әдістер талқыланады және ұсынылады. Оларға 6-бөлікте баяндалған тәуекелдерді бағалаудың әр түрлі нысандары мен Қосымшаларда тәуекелдерді бағалаудың әр түрлі мүмкіндіктерін толық баяндауды қоса алғанда 5-бөлікте баяндалған тәуекелдерді бағалаудың процестері жатады. Сондықтан GMITS стандартының 3-бөлігі аталған тақырыптарға, әсіресе тәуекелдерді бағалауды қалай орындау керектігі туралы барынша егжей-тегжейлі ақпарат алу үшін пайдаланылуы мүмкін.

GMITS. 4-бөлім. Қауіпсіздікті қамтамасыз ету шараларын таңдау

GMITS стандартының 4-бөлігінде бағалаудың әр түрлі әдістеріне қатысты басқарудың құралдарын таңдау туралы ақпараттар (мысалы 4-бөлімде баяндалған сияқты) келтірілген. 4-бөлім

ҚР СТ ИСО/МЭК 17799 сияқты нақты нұсқаулардың ішінен басқару құралдарын таңдаған кезде, сондай-ақ тәуекелдерді бөлшектеп бағалауға сәйкес басқару құралдарын таңдаған кезде көмектесуі мүмкін. Бұл бөлікті осы стандарттың 5-бөлігінде баяндалған басқару құралдарын таңдаған кезде пайдаланылуы мүмкін.

GMITS. 5-бөлім. Сыртқы біріктіру үшін қауіпсіздікті қамтамасыз ету шаралары

GMITS стандартының 5-бөлігінде өзінің ақпараттық жүйелерін сыртқы желілерге қосатын ұйымдар үшін нұсқаулықтар келтіріледі. Бұл бөлікте осы қосулармен қолдау табатын сыртқы қосулар мен сервистер үшін қауіпсіздікті қамтамасыз етуге мүмкіндік бертін қауіпсіздікті басқару құралдарын таңдау мен пайдалану сипатталады. Бұған қоса онда қажеттілік осы қосулармен шартталған басқарудың қосымша құралдары сипатталады. 5-бөлік сондай-ақ егер сыртқы қосылулар пайдаланылса, *ҚР СТ ИСО/МЭК* 17799 стандартынан қауіпсіздікті басқару құралдарын таңдаған кезде пайдаланылуы мүмкін.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ ИСО/МЭК 17799-2006 Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпаратты қорғауды басқару бойынша ережелер жинағы.

ҚР СТ ИСО/МЭК 27001 -2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар.

3 Терминдер мен анықтамалар

Осы стандартта [1], [9], *ҚР СТ ИСО/МЭК 17799*, *ҚР СТ ИСО/МЭК 27001* бойынша терминдер, сондай-ақ сәйкес анықтамаларымен мынадай терминдер қолданылады.

Ақпарат (information): Осы деректерге қолданылатын шартты келісімдер арқылы осы сәтте деректерге берілген мағыналық мәні.

Ақпараттық қауіпсіздік саясаты (information security policy): Сындарлы ақпараттарды қоса алғанда, ресурстардың қалайша басқарылатынын, қорғалатыны мен таратылатынын анықтайтын ережелер, нұсқаулар мен нақты нормалар.

Ресурс (asset): Ұйым, оның бизнес-операцияларына және олардың үздіксіздігі үшін құндылық беретіннің барлығы.

Қауіпсіздікті басқару құралдары (security control): Қауіпсіздіктің тәуекелдерін азайтуға мүмкіндік беретін нақты нормалар (practice), рәсімдер немесе тетіктер.

Ақпараттық қауіпсіздікті басқару (information security management): Ақпараттық қауіпсіздікті іске асыруға мүмкіндік беретін механизмді ұсыну.

Ескертпе – Тәуекелдерді басқару әдетте тәуекелдерді бағалауды, тәуекелдерді өңдеуді, тәуекелдерді қабылдауды және тәуекелдерді тапсыруды қамтиды.

4 Негізгі ережелер

4.1 Ақпараттық қауіпсіздік негізі

Ақпараттық қауіпсіздіктің мақсаты бизнестің үздіксіздігі мен ақпараттық қауіпсіздікке қақтығыстардың әсерін алдын алу мен азайту көмегімен бизнестің зиянын азайтуға қамтамасыз етуден тұрады.

Ақпараттық қауіпсіздікті басқару ақпаратты ұжымдық пайдалануға, ақпаратты ұжымдық пайдалануға бұл ретте ақпараттарды және АҚБЖ-ны қолдану саласындағы шектерде барлық өзге ресурстарды қорғауды қамтамасыз ете отырып, мүмкіндік береді (сонымен қатар 5.1-бөлімді қараңыз.). Ақпараттық қауіпсіздік 3 негізгі компоненттерді қамтамасыз етуі тиіс

– Құпиялылық: маңызды ақпаратты авторизацияланған жариялаудан және оқылатын түрдегі ақпаратты ұстап қалудан қорғау;

– Тұтастық: дәлдікті қорғау және ақпараттың толықты және бағдарламалық қамтамсыз ету.

– Қол жетімділік: пайдаланушылар үшін ақпараттың қол жетімділігін және маңызды сервистерді қамтамасыз ету.

Ақпарат көптеген нысандарға ие. Ол компьютерде сақталуы, желілер арқылы берілуі, қағазда басылуы немесе жазылуы немесе сөйлем түрінде айтылуы мүмкін. Қауіпсіздікті қамтамасыз ету тұрғысынан қажетті қорғау баспалық құжаттарды, деректер базасын, үлдірлерді, тұсау кесерлерді, магниттік ленталарды, дискеталарды, компакт-дискілерді, сөйлесулерді, (мысалы: стационарлық және ұтқыр телефондар сияқты технологияларды пайдалану арқылы сөйлесулер) және барлық басқа әдістер мен білім мен ой-пікірлерді беру үшін пайдаланушы ақпарат тасығыштарды қоса алғанда, ақпараттың барлық нысандарына қолданылуы тиіс.

4.2 Шаралар қабылдану қажеттігі

Ұйымға тиесілі ақпараттар, сондай-ақ жүйелер осы ақпаратты қолдайтын қосымшалар мен желілер маңызды бизнес-ресурстар болып

табылады. Ресурстардың құпиялылығы, тұтастығы мен қол жетімділігі бәсекеге қабілеттілікті, ақша қаражатының ағынын, рентабельділігін, құқықтық талаптар мен коммерциялық репутацияларға сәйкестігін қолдау үшін үлкен маңызға ие болуы тиіс. Ұйым әр түрлі көздерден қауіпсіздіктің қауіптерінің санының ұлғаюына ұшырауы мүмкін. Ұйымға тиесілі жүйелер, қосымшалар мен желілер, компьютерлерді, қарақшылықты, зымияндықтарды, вандализмдерді, қолдану мен алаяқтықты және жұмыстағы басқа да бас тарту көздерін немесе апаттарды қоса алғанда, елеулі қауіптер (5.3-бөлімді қараңыз) қатарының мақсаты болуы мүмкін. Компьютерлік вирустар мен компьютерлік хакерлерден кең талқыланатын қауіптер сияқты жаңа мүмкін болатын залал көздері туындауда. Осындай ақпараттық қауіпсіздік тартылатын қауіптер барынша таратылатын, барынша наразылық тудыратын, әбден жетілдендірілген болады. Дәл сол уақытта ақпараттық жүйелер мен сервистерге негізделген технологияларға ұлғайған тәуелділіктің нәтижесінде ұйым қауіпсіздік қауіптеріне анағұрлым осал болуы мүмкін.

Желілік технологияларды барынша кең пайдалану компьютерлік желілерге авторизацияланған ену үшін жаңа мүмкіндіктер береді, ал есептеуіш техниканың таралуына үрдістер ұйымның АҚБЖ-сын орталықтандырып бақылау мамандары жүзеге асыратын әрекеттер аясын қысқартады.

Осындай қауіптерді бейнелеу үшін ұйымға тиесілі ақпараттарды қорғауды қамтамасыз етуге мүмкіндік беретін тиісті басқару мақсаттары мен басқару құралдарын сәйкестендіру және іске асыру үшін қажет. Бұған қатысты *ҚР СТ ИСО/МЭК 17799 және ҚР СТ ИСО/МЭК 27001* стандарттары осы талапты орындау үшін және ақпараттық қауіпсіздікті басқару жүйелерін әзірлеу үшін басқару құралдарының жақсы көзін ұсынады. Ұйым қажетті басқару құралдарын сәйкестендіру және таңдау үшін өзінің қауіпсіздік талаптарын (5.3 және 5.4-бөлімдерін қараңыз) АҚБЖ-ға, өз бизнес процестерінің және қосымшаларының мәтініне енгізілген ақпараттық жүйелерге сәйкестендіруі тиіс.

Қауіпсіздік қауіптеріне көп ұлтты корпорациялардан бастап, орта және шағын бизнес кәсіпорындарына дейін барлық қызмет түрлеріндегі және барлық мөлшердегі ұйымдар осал болады. Ұйымға тиесілі ақпараттарды қорғау жөніндегі шаралар қаншалықты жылдам қабылданса, соншалықты уақыт өте келе ұйымның қауіпсіздігі арзан әрі барынша тиімді болмақ.

4.3 Тәуекелдерді бағалау процесі туралы жалпы ұсыным

Әдетте тәуекелдерді бағалау құралдары мен әдістерді барлық АҚБЖ-ға немесе нақты ақпараттық жүйелерге және техникалық құралдарға қолданылады. Бірақ, сондай-ақ егер де бұл оңтайлы, нақты және пайдалы

болып табылса, олар жекелеген жүйелік компоненттерге немесе сервистерге бағытталатын болады. Тәуекелдерді бағалау мынадай аспектілердің жүйелік талдауын қамтиды.

– **Салдар** – бизнес үшін жоғалтудың мүмкін болатын салдарын немесе ақпараттардың құпиялылығын, тұтастығын және қол жетімділігін жеткіліксіз қамтамасыз етуді ескере отырып, ақпараттық қауіпсіздікті елеулі бұзушылық нәтижесінде туындауы мүмкін залал:

– **Ықтималдық** – осындай бұзушылық қауіптерді, осалдықтар мен басқару құралдарын түрлендіру аясында болып жататын нақты ықтималдық.

Бұл процес:

– Осы АҚБЖ, талаптарды бизнес-ақпараттардың қауіпсіздігіне, құқықтық және нормативтік талаптарға, сәйкестендіру үшін лайықты тәуекелдерді (6-бөлімді қараңыз) бағалау, сондай-ақ тәуекелдерді қабылдау мен тәуекелдердің оңтайлы деңгейлерін сәйкестендіру үшін өлшемдерді айқындау әдісін таңдау.

– АҚБЖ-ға енгізілген ақпараттық қауіпсіздікті басқару жүйелері (жүйесі) және ақпараттық жүйелер үшін тәуекелдерді (5-бөлімді қараңыз) сәйкестендіру және бағалау; тәуекелдерді өңдеу нысандарын сәйкестендіру және бағалау, тәуекелдерді оңтайлы деңгейлерге дейін азайту үшін басқару мақсаттары мен басқару құралдарын таңдау, сондай-ақ – сертификаттау үшін = қолданушылық туралы ереже дайындау.

Қауіпсіздікті басқарудың баламалық құралдарын іске асыруды қалайтын әрбір ұйым ақпараттық қауіпсіздіктердің тәуекелдерін басқару үшін әрекеттерді өңдеу мен басымдықтарды айқындау жөніндегі қажетті әрекеттерді айқындау үшін тәуекелдерді бағалау нәтижелерін пайдалануы тиіс. Осы процес *ҚР СТ ИСО/МЭК 17799* немесе *ҚР СТ ИСО/МЭК 27001* стандарттардан, тиісінше А-қосымшасынан басқару құралдарын тиісті іске асыру мен қолдануды ұйымның сәйкестендіруіне мүмкіндік береді. Тәуекелдердің бағалау мынадай факторларға қатысты:

– Бизнес ақпараттар мен жүйелердің үлгісі;

– Осы ақпарат пайдаланылатын қызметтердің мақсаттары;

– Жүйе пайдаланылатын және жұмыс істейтін қоршаған орта;

– Іске асырылатын басқару құралдарымен қамтамасыз етілген қорғау.

Тәуекелдерді бағалау процесінде *ҚР СТ ИСО/МЭК 27001* стандартында келтірілген ұсынымдарға қосымша барынша қуатты басқару құралдарын іске асыруды талап ететін қауіпсіздіктің айрықша қауіпсіздігімен сәйкестендірілуі мүмкін. Осы басқару құралдарын таңдау тәуекелдерді бағалау нәтижелерінің негізінде негізделуі тиіс. Ақпараттық қауіпсіздіктерді басқару құралдарына шығыстар ақпараттардың және тәуекелдерге тартылатын басқа бизнес-ресурстардың коммерциялық бағалылығына сәйкес болуы тиіс. Сонымен қатар осы шығыстар

қауіпсіздікті бұзушылықты жасауы мүмкін бизнестің әсерлеріне қатысты теңгерілген болуы тиіс. Сондықтан да бизнес талаптар мен басымдықтардың өзгерістерін есептеуге мүмкіндік беретін бизнес тәуекелдер мен қауіпсіздіктерді басқару құралдарының мерзімдік талдауы ақпараттық қауіпсіздікті басқарудың тұрақты пайдаланылатын функциясы болып табылады.

Тәуекелдерді бағалау және тәуекелдерді басқару үшін қажетті ресурстар жүргізілетін талдаудың тереңдігіне, қауіпсіздіктің талаптарына және ұйым бизнесінің күрделілігіне қатысты ажыратылуы мүмкін.

Тәжірибе көрсеткендей мынадай факторлар ұйымдағы ақпараттық қауіпсіздікті сәтті іске асыру үшін сындарлы болып табылуы мүмкін.

– Бизнестің мақсаттары мен талаптарына негізделетін және ұйым басшылығы орындайтын қауіпсіздік мақсаттары мен әрекеттері:

– Жоғары басшылық тарапынан айқын қолдау мен ден қоюшылық (мүдделілік);

– Қауіпсіздік тәуекелдерін жақсы түсіну;

– Қауіпсіздікті менеджер мен қызметкер деңгейіне дейін тиімді жылжыту;

– Барлық қызметкерлер мен мердігерлерге дейін ақпараттық қауіпсіздік стандарттары мен саясаты жөніндегі барлығын қамтитын нұсқаулықтарды тарату.

4.4 ЖІБТ (PDCA) моделдерінде тәуекелдерді бағалау мен тәуекелдерді өңдеу

АҚБЖ процесінде орындалуы тиіс ЖІБТ моделі мен әрекетіне көзқарас кезінде ЖІБТ моделдерінің шеңберінде «жоспарлау» кезеңінің басты бөлігі болып табылады. Тәуекелдерді өңдеу ЖІБТ моделдері «іске асыру» кезеңінің маңызды бөлігін құрайды. Егер ұйым сертификаттауға өтінім беруге шешім қабылдайтын болса, онда мұны «іске асыру» кезеңінің барлық әрекеттерін орындағаннан кейін ғана жасау керек.

Бірақ бұл мүмкін, бірақ айқын емес болса да «бағалау» кезеңінде барлық іске асырылған басқару құралдары тәуекелдерді тиімді азайтатындығын енгізілетіндігін ескеру қажет. «Түзету» кезеңіндегі әрекеттердің жартысы осы кезеңді «Іске асыру» кезеңіне ұқсастыратын қайтадан бағаланған тәуекелдерді өңдеу сияқты өзгешелікті білдіреді. Бұл осы стандартта одан әрі сипатталатын тәуекелдерді бағалауды және тәуекелдерді өңдеу ЖІБТ моделдерінің барлық кезеңдерін қолдауға көмектеседі.

5 Тәуекелдерді бағалау процесі

Тәуекелдерді бағалау мынадай кезеңдерден тұрады:

– Ресурстардың құндылықтарын сәйкестендіру мен айқындау (5.1 және 5.2-тармақтарын қараңыз);

– Барлық қауіпсіздік талаптарын, яғни қауіптер мен осалдықтар, құқықтық және бизнес талаптарын сәйкестендіру (5.3-тармағын қараңыз);

– Қауіптер мен осалдықтардың ықтималдылығын бағалау, сондай-ақ құқықтық және бизнес талаптардың маңыздылығын бағалау; (5.4-тармағын қараңыз);

– Аталған факторлар нәтижесінде туындаған тәуекелдерді есеп (5.5-тармағын қараңыз);

– Тәуекелдерді өңдеудің қажетті нұсқасын таңдау (5.6-тармағын қараңыз);

– Тәуекелдердің оңтайлы деңгейге дейін төмендеуі үшін басқару құралдарын таңдау (5.7-тармағын қараңыз).

5.1 Ресурстарды сәйкестендіру

Ұйым, оның бизнес операциялары мен олардың үздіксіздігіне құндылық пен пайдалылыққа ие болатын қандай да бір нәрсе ресурс болып табылады. Сондықтан ресурстарға бизнес операциялар мен бизнестің үздіксіздігін түзу орындайтын дұрыс орындауды қамтамасыз етуге мүмкіндік беретін қорғау талап етеді. Ресурстарға тиісті басқару және оларды есепке алу[2] ұйымның ресурстарының қауіпсіздігін қолдау үшін маңыздырақ мәнге ие. Бұл екі аспекті басқарудың [2] барлық деңгейлерінде басты міндеттеме болуы тиіс. Түгендеу кезінде негізгі ресурстардың ескерілуі маңызды. Қалып қойылған немесе ұмытылған ресурстардың жоқтығына сенімді болу үшін бизнестің, ұйымдардың, оның орналасқан жерінің, ресурстары мен технологияның мінездемелерінің терминдерінде қаралатын АҚБЖ-ның қолдану саласын айқындаған жөн.

Осы қолдану саласының шекараларында әрбір ресурс анық түрде сәйкестендірілген және тиісті түрде бағаланған болуы тиіс (5.2 – бөлімінің төменгі жағын қараңыз), ал оның иесі мен қауіпсіздік санаты келісілген және құжаттандырылған болуы тиіс ([6]/[7], *ҚР СТ ИСО/МЭК 17799* қараңыз). Ресурстарға мысалы, мыналар:

– **Ақпараттық ресурстар***:* деректер базасы мен деректер файлы, жүйелік құжаттама, пайдаланушының нұсқаулығы, оқу материалы, пайдалану және қолдау рәсімдері, үздіксіз қызметті қамтамасыз ету жоспарлары, апаттық қалпына келтіру құралдары;

– **Баспалық құжаттар***:* келісім шарттар, нұсқаулық, компанияның құжаттамасы, маңызды бизнес нәтижелерімен құжаттар ;

– **Бағдарламалық ресурстар***:* қолданбалы бағдарламалық қамтамасыз ету, жүйелік бағдарламалық қамтамасыз ету, әзірлеу және жою құралдары;

– **Физикалық ресурстар***:* есептеуіш жабдықтары мен байланыс аппаратурасы, ақпараттарды магниттік тасығыштар (таспалар мен дискілер), басқа да техникалық жабдықтар (қоректендіру көздері, желдеткіштер), жиһаз, үй-жайлар;

– **Адамдар:** персоналдар, тапсырыс берушілер, абоненттер;

– **Компаниялардың бет-бейнелері мен беделі**;

– **Сервистер және қызметтер***:* есептеуіш және коммуникациялық сервистер, басқа да техникалық қызметтер (жылу беру, жарық беру, электрлік қоректендіру, желдету).

5.1-кезеңінің нәтижелері:

Осы кезеңнің нәтижесі қаралатын АҚБЖ-ға, оның орналасқан жеріне және оның иесіне жататын барлық негізгі ресурстар көрсетілуі тиіс тізілім болуы қажет.

5.2 Ресурстарды бағалау

Ұйымның бизнес тұтынушылығына негізделген ресурстарды сәйкестендіру мен бағалау тәуекелдерді ең басты құрастырушы бағалау болып табылады. Ресурстар үшін қажетті қорғауды сәйкестендіру үшін олардың бизнес үшін маңыздылығы негізінде олардың құндылығын және белгілі бір жағдайларда олардың әлеуметтік маңыздылығын айқындау қажет. Бұл маңыздылық әдетте бизнеске әлеуетті әсер ету терминдерінде айқындалады, олар ашу, модификация, ақпараттардың қол жетімділігі және/немесе жою және басқа ресурстар сияқты қаламаған қақтығыстар нәтижесінде болу. Бұл қақтығыстар өз кезегінде қаржылық шығындарға, табыстың, нарықтағы үлестің азаюына немесе компания беделінің зиянының әкеп соғуы мүмкін. Ресурстарды бағалау үшін кірістерін ұйым мен оның бизнесі үшін ресурстардың, әсіресе, ақпараттардың маңыздылығы туралы беделді түрде хабарлауға қабілетті ресурстардың иелерімен пайдаланушылары ұсынуы тиіс.

Алынған бағалар ресурстардың сатып алу құны мен қолдау құнына, ұйымның бизнеске арналған құпиялылықты толықтық пен қол жетімділікті жоғалтуы мүмкін іс әрекеттерге қатысты болуы тиіс. Ресурстардың құндылығын біртұтас түрде айқындау және осы бағаларды тиісті түрде байланыстыру үшін ресурстардың бағалау шәкілін қолдану қажет.

Әрбір ресурс үшін құпиялылықты, толықтықты немесе қол жетімділікті бұзған жағдайда және кез келген ресурстің басқа маңызды

қасиетін бұзған жағдайда бизнеске әсер ететін құндылық сәйкестендірілген болуы тиіс. Осы тәрізді шәкіл ретінде бағалауға, мысалы:

– Төменгі, орта және жоғары деңгейлер арасындағы айырмашылық;

– Неғұрлым толық шәкіл: төменгі – орта – жоғары - өте жоғары;

Ұйым ресурстарды бағалау шәкілі үшін өзінің жеке шекараларын белгілеуі тиіс. «Төмен» немесе «жоғары» деңгейдің зияны деп саналатын шешім шағын ұйым үшін апат болуы мүмкін немесе тіпті өте ірі ұйым үшін де зиянды болатын тек ұйымға ғана залал болып табылады.

Ұйымның бизнес терминдерінде осы бағаларды дұрыс және ұғымды түсіндіру ресурстарды бағалау үшін кіріс деректерін алу мақсатында жасалуы тиіс иеленушілер мен пайдаланушылардың әңгімелесуі кезінде аса маңызды.

5.2-Кезеңнің нәтижесі:

Осы кезеңнің нәтижесінде ресурстардың тізіліміне сәйкестендірілген әрбір ресурс үшін әрбір өлшем бойынша баға қосылуы тиіс, мысалы, құпиялылық, толықтық және қол жетімділік, сондай-ақ, егер олар пайдаланылса кез келген басқа өлшемдер бойынша.

5.3 Қауіпсіздік талаптарын сәйкестендіру

5.3.1 Талап көздері

Кез келген ұйымдағы қауіпсіздік талаптары мөлшеріне қатысты емес, шындығында АҚБЖ-да құжатталуы тиіс үш негізгі көздерден туындайды:

– Туындауы бизнестегі елеулі шығындарға әкелуі мүмкін қауіптер мен осалдықтардың бірегей жиынтығы;

– Ұйымның олардың сауда серіктестері, мердігерлерінің және қызметтерді жеткізушілерінің орындалуы тиіс құқықтық талаптары мен шарттық міндеттемелері;

– Ұйымның бизнес-операциялар мен бизнес-процестерді қолдау үшін және ұйымның ақпараттық жүйелеріне қолдану үшін әзірленген ақпараттарды өңдеу жөніндегі қағидаттарды, мақсаттардың және талаптардың бірегей жинағы.

Аталған қауіпсіздік талаптарын сәйкестендіргеннен кейін оларды құпиялылық, толықтық және қол жетімділік талаптарының терминдерінде құрастырған пайдалы.

Кейбір сәттерде – тәуекелдерді бағалау жөніндегі әрекеттердің басталуына дейін, не осы кезеңнің алдында – іске асырылған қауіпсіздікті басқару құралдарын сәйкестендіру қажет. Бұл қауіптер мен осалдықтарды толық сәйкестендіру мен шынайы бағалау үшін талап етіледі, сондай-ақ бұған дейін қолданыстағылар мен жақсы өзара әрекет ететін басқарудың қосымша құралдарын таңдау үшін маңызды (5.6-кезеңін де қараңыз). Осы

стандарт *ҚР СТ ИСО/МЭК* 17799 және *ҚР СТ ИСО/МЭК 27001* стандарттарына қатысты қолданыстағы қауіпсіздік жағдайын тексеруге мүмкіндік береді.

5.3.2 Қауіптер мен осалдықтарды сәйкестендіру

Ресурстар әр түрлі үлгідегі қауіптерге тартылады. Қауіп жүйеге немесе ұйымға және оның ресурстарына зиянның себебі болуы мүмкін қаламаған қақтығысқа әкеп соғуға қабілетті. Бұл зиян ұйымға тиесілі ақпаратқа тікелей немесе тікелей емес шабуыл нәтижесінде мысалы, ақпараттарды авторизацияланған жою, оны ашу, модификация, бөліну, сондай-ақ қол жетімсіздік немесе жоғалту нәтижесінде туындауы мүмкін. Қауіптер кездейсоқ немесе әдейі жасалған көздер немесе оқиғалардың себебі бойынша туындауы мүмкін. Ресурстарға зиян келтіру үшін қауіп ұйымдар пайдаланатын жүйелердің, қосымшалардың немесе сервистердің қандай да бір осалдықты пайдалануы қажет (төмен қараңыз). Қауіптің мысалдары осы стандарттың А.1 және А.2 қосымшаларында келтірілген, ал GMITS 3-бөлігінде және «Protecting Business Information» («Бизнес ақпараттарды қорғау») ([8] және [9] қараңыз) басылымында қауіптер туралы қосымша ақпарат келтірілген.

Осалдықтар ұйымның ресурстарымен байланысты әлсіз жақтарын көрсетеді. Осы әлсіз жақтар осы ресурстарға жоғалуға, бөлінуге немесе зиян келтіруге әкелуі мүмкін қауіптер пайдалануы мүмкін. Осалдық өз бетінше зиян келтіре алмайды, бұл қауіпке ресурстарға әсер етуге мүмкіндік беретін қарапайым шарттар немесе шарттардың қатары. Осалдықтарды сәйкестендірген кезде бизнеске және ресурстармен мыналарда:

– Физикалық ортада,

– Персоналдармен, басқарумен және әкімшілік етумен байланысты басқару рәсімдерімен құралдарында,

– Аппараттық және бағдарламалық қамтамасыз етуде, байланыстың жабдықтары мен құралдарында байланысты ресурстар мен олар қолдайтын бизнеске зиян келтіру мақсатында қауіптің көзі ретінде пайдаланылуы мүмкін әлсіз орындарды сәйкестендірген жөн.

Осалдық мысалдары осы стандарттың А.3 қосымшасында келтірілген, ал [3] басылымында осалдықтар туралы қосымша ақпарат келтірілген.

Мынаған назар аударыңыз: тәуекелдерді бағалаудың пайдаланылған әдісіне қатысты қауіптер мен осалдықтар бірге немесе жеке бағаланады. Екі нұсқаны да пайдалану және оларды таңдау туралы шешу мүмкіндігін тәуекелдерді бағалаулардың жалпы тәсілдерін таңдаған кезде қабылдаған жөн (сондай-ақ 6-бөлімді және Б.2-қосымшасын қараңыз).

5.3.3 Құқықтық, нормативтік талаптары мен шарттық міндеттемелер

АҚБЖ-ға ұйым, оның сауда серіктесі, мердігерлер және қызмет жеткізушілер орындалуы тиіс құқықтық талаптар мен шарттық міндеттемелердің жиынтығымен байланысты қауіпсіздік талаптары құжаттануы тиіс. Осы талаптарды АҚБЖ-ның қолдауы үлкен маңызға ие, мысалы, патенттелген бағдарламалық қамтамасыз етуді көшіруге ұйымның құжаттарын қорғауға немесе деректерді қорғауға бақылауды жүзеге асыру үшін. Әрбір ақпараттық жүйелерде қауіпсіздіктерді басқару құралдарының бар болуының немесе жоқтығы құқықтық немесе азаматтық міндеттемелердің ешқайсысын, сондай-ақ коммерциялық шарттардың бірде біреуін бұзбағаны аса маңызды. Сондықтан әрбір ресурсқа байланысты құқықтық талаптар мен шарттық міндеттемелерді сәйкестендіру қажет.

5.3.4 Ұйымның қағидаттары, мақсаттары мен бизнес-талаптары

Бұған қоса АҚБЖ-да ұйымның бизнес-операцияларды қолдау мақсатында аппараттарды өңдеу үшін барлық ұйымдарда қолданылатын қағидаттармен, мақсаттармен және талаптармен байланысты қауіпсіздік талаптары құжаттандырылған болуы тиіс. Осы талаптардың АҚБЖ-сын қолдау бәсекелестік қабілеттілікті, ақша ағынан және/немесе рентабельділікті арттыру үшін үлкен маңызға ие. Әрбір ақпараттық жүйелерде қауіпсіздікті басқару құралдарының болуы немесе болмауы бизнес-операциялары тиімді орындауға кедергі болмауы аса маңызды. Сондықтан әрбір ресурс үшін онымен байланысты бизнес мақсаттары мен бизнес талаптарын сәйкестендіру қажет.

5.3-Кезеңнің нәтижесі:

5.1 кезеңінде сәйкестендірілген әрбір ресурс үшін 5.3-кезеңінің нәтижесінде сәйкестендірілген қауіптер мен осалдықтары, құқықтық талаптар/шарттық міндеттемелер және бизнес талаптардың тізімі құрастырылған болуы тиіс.

5.4 Қауіпсіздік талаптарын бағалау

Ресурстарды бағалаған кездегі сияқты қауіпсіздік талаптарын бағалаған жағдайда тәуекелдерді бағалаудың пайдаланылатын әдісіне сәйкес келетін осы бағалау үшін шәкілді анықтау қажет (сондай-ақ 6-бөлімді қараңыз). Көптеген жағдайларда осы процесті мүлдем қиындатпау үшін қарапайым үш деңгейлі шәкілді пайдалану жеткілікті, мысалы:

– Төменгі деңгей
– Орта деңгей
– Жоғарғы деңгей.

5.4.1 Қауіптер мен осалдықтарды бағалау

Қауіптер мен осалдықтарды сәйкестендіргеннен кейін қауіптер мен осалдықтардың кейбір үйлесімінде іске асырудың шынайылығын бағалау қажет.

Мынаған назар аударыңыз: қауіптер мен осалдықтардың бірге немесе жеке, қалай бағаланатындығына қатысты қауіптер мен осалдықтарды жеке бағалауды немесе бірлескен бағалауды пайдаланған жөн.

Қауіптің ықтималдылығын бағалаған кезде мыналарды назарға алған жөн:

– Қасақана қауіп үшін: ынталандыру, қабылданған және талап етілетін мүмкіндіктер, әлеуетті тәртіп бұзушыларға қол жетімді ресурстар, және ресурстардың тартымдылығын түсіну;

– Кездейсоқ (қасақана) қауіптер үшін: тәжірибеге, статистикаға және т.б. сәйкес олар қаншалықты жиі туындауы мүмкін; химиялық және мұнай өндіруші зауыттарға жақындық сияқты географиялық факторлар, шұғыл табиғат жағдайларының ықтималдық орасан аудандарда болу; және адам қателерін көрсетуі мүмкін факторлар және жабдықтың жұмысқа қабілеттілігін бұзу.

Қақтығыстың пайда болу толық ықтималдылығы сондай-ақ ресурстардың осалдығына қатысты, яғни оларды қаншалықты жеңіл пайдалануға болатындығына байланысты. Ізінше осалдықтар бірнеше шәкілдер бойынша бағалануы тиіс, мысалы мыналар:

– Жоғары ықтимал немесе – осы ықтималдықты пайдаланған өте жеңіл, қорғау жоқ немесе өте әлсіз;

– Мүмкін болатын – осалдық пайдаланылуы мүмкін, алайда қорғауға ие;

– Өте аз ықтимал немесе мүмкін болатын – осы осалдықта пайдалану қиын, жақсы қорғауға ие.

Қауіптер мен осалдықтарды бағалау үшін пайдаланылатын ақпараттар қаралатын АҚБЖ-ға және тиісті бизнес-процесстерге қатынасы бар адамдардан алынған болуы мүмкін. Бұлар, мысалы, кадр бөлімінің қызметкерлері, жоспарлау жөніндегі мамандар және АТ мамандары, сондай-ақ қауіпсіздік үшін ұйымға жауап беретін адамдар. Бұған қоса қауіптер мен осалдықтардың тізімдерін (мысалға А қосымшасында және [3]), сондай-ақ осы стандарттың А қосымшасында келтірілген ҚР СТ ИСО/МЭК 17799 стандартынан басқарудың қауіптері мен құралдардың арасындағы байланыс.

5.4.2 Құқықтық талаптар мен бизнес-талаптарын бағалау

Қауіптер мен осалдықтар бағаланған сияқты енді құқықтық талаптар мен бизнес-талаптар үшін бағаларды айқындаған жөн (5.3.3 және 5.3.4 – тармақтарын қараңыз). Бұл осы қауіпсіздік талаптармен байланысты тәуекелдегі есептеу үшін қажет

Қандай да бір құқықтық немесе бизнес-талаптарға бағаларды белгілеу үшін мыналарды айқындау қажет:

– Осы құқықтық талаптарды/шарттық міндеттемелерді немесе бизнес талаптарды орындамаған жағдайда бизнеске әсер ету қаншалықты байыпты болады;

– Бұл қаралатын ресурстар мен барлық АҚБЖ үшін қандай сардарларға қатысты болады; және

– Бұның болатындығына ықтималдық қандай.

Аталған факторларды талдау нәтижелері әрбір ресурс және әрбір құқықтық талаптар/шарттық міндеттемелер және әрбір бизнес талаптар үшін қауіпсіздік талаптарына арналған бағалар шәкілінде тиісті бағаны айқындау үшін пайдаланған жөн.

5.4-кезеңінің нәтижесі:

Осы кезең нәтижесінде барлық сәйкестендірілген қауіпсіздік талаптарына кейбір бағалар берілуі тиіс (5.3 кезеңінен жоғары қараңыз).

5.5 Қауіпсіздік тәуекелдерінің есебі

Тәуекелдерді бағалаудың мақсаты 5.1-5.4 кезеңдерінде алынған нәтижелердің негізінде тәуекелдерді сәйкестендіру мен бағалауда көрінеді. Бұл тәуекелдер Ресурстардың бағалары мен бағаланған деңгейі тиісті қауіпсіздік талаптарын үйлестіруден есептелінеді.

Мынадай: мысалы, активтерге, осалдықтар мен қауіптіліктерге, сондай-ақ құқықтық және бизнес-талаптарға тағылған бағалар сияқты факторларды байланыстыруға мүмкіндік беретін түрлі әдістер қолданылады, нәтижесінде тәуекел деңгейінің мәні алынады. Осы мәндерді алудың бірнеше әртүрлі әдістері «тәуекелдерді бағалау әдісінің үлгілері мен мысалдары» Б.2 қосымшасында сипатталады. Бұл әдістер 3 бөлімде сипатталған ұғымдарға негізделеді.

Алдыңғы бөлімдерде сипатталған ұғымдар кейбір мағыналық түрде бірігетіндігі және тек ұйымның өзі ғана оның бизнес талаптары мен оның қауіпсіздік талаптарына келетін тәуекелдерді бағалаудың қандай әдісі туралы шешім қабылдауы мүмкін шартында тәуекелдерді бағалаудың «дұрыс» немесе «дұрыс емес» тәсілдерінің жоқ екендігін атап өту маңызды.

5.5 кезеңінің нәтижелері:

Қаралатын АҚБЖ-ның қолдану саласында тұрған әрбір ресурс үшін осы кезең нәтижесінде ашылу, модификация, қол жетімділік және жою нысанында пайда болатын әрбір іс әрекет үшін өлшенген тәуекелдердің тізімі құрастырылатын болуы тиіс.

5.6 Тәуекелдерді өңдеу нысандарын сәйкестендіру және бағалау

Тәуекелдеу сәйкестендірілген және бағаланғаннан кейін ұйымның келесі міндеті осы тәуекелдерді өңдеу үшін сәйкес келетін әрекеттің өзін сәйкестендіру және бағалау болып табылады. Бұл шешім қамтылған ресурстар туралы ақпараттар, сондай-ақ бизнеске әсер ету негізінде қабылдануы тиіс. Осы шешімнің негізіне жататын тағы бір маңызды фактор тәуекелдерді бағалаудың қажетті әдісін таңдаудан кейін сәйкестендірілген тәуекелдің оңтайлы деңгейі болып табылады (6 бөлімді қараңыз).

Сәйкестендірілген және бағаланған тәуекелдер үшін (5.1 - 5.5 кезеңдерінде сипатталған іс әрекеттердің нәтижесінде) Ұйым қолдануы мүмкін болатын әрекеттердің төртеуі құралады:

– Осы тәуекелдерді азайту үшін тиісті бағалау құралдарын қолдану. (5.7 бөлімінің төменгі жағын қараңыз);

– Олар ұйымның саясаты мен тәуекелдерді қабылдау өлшемдеріне нақты қанағаттандыратыны жағдайында тәуекелдерді әдейі және қасақана қабылдау (6- бөлімді қараңыз);

– Тәуекелдердің алдын алу (5.6.1 бөлімінің төменгі жағын қараңыз);

– Қауымдастырған бизнес тәуекелдерді басқа тараптарға беру (5.6.2 бөлімінің төменгі жағын қараңыз).

Аударылған нысандар барынша сәйкес келетін нысандарды айқындау мақсатында әрбір тәуекел үшін бағаланған болуы тиіс.

5.6.1 Тәуекелдердің алдын алу

Тәуекелдердің алдын алуға нәтижесінде ресурстар тәуекелденген салалардан алынып тасталатындай барлық іс әрекеттер жатады (мысалы, физикалық салалар немесе бизнес-процесстер). Оған, мысалы, мынадай түрде қол жеткізуге болады:

– Жекелеген бизнес операцияларды орындамау (мысалы, электронды коммерция құралдарын пайдаланбау немесе нақты бизнес операциялары үшін Интернет желісін пайдаланбау);

– Тәуекелге тартылған салалардың ресурстарды ауыстыру (мысалы, ұйымның Интернет желісінде маңызды файлдарды сақтауға немесе тиісті физикалық қорғауы жоқ салалардың ресурстарды ауыстыруына тиым салынады);

– Егер қорғаудың тиісті қамтамасыз етілуі кепілдендірілмеген болса, мысалы, үшінші тараппен аса маңызды ақпаратты өңдемеуге шешім.

Тәуекелдердің алдын алудың нысанын бағалау кезінде оларды бизнес-қажеттіліктер және қаржы шығындары теңгерімделген болуы қажет. Мысалы, электронды коммерция үшін Интернет желісін пайдалану хакерлермен байланысты барлық проблемаларға қарамастан бизнес қажеттілігінің міндетті салдары болуы мүмкін, ал ресурстарды барынша

қауіпсіз орындарға ауыстыру бизнес-процесінің тұрғысынан алғанда жол берілмеуі мүмкін. Бұндай ұқсас жағдайларда басқа әдістерді, яғни тәуекелдерді беру мен тәуекелдерді азайтудың басқа әдістерін қараған жөн.

5.6.2 Тәуекелдерді беру

Егер тәуекелдерді алдын алу мүмкін емес және тәуекелдерді азайтуға қол жеткізу қиын, немесе мүлдем қымбат болған жағдайда тәуекелдерді беру ең жақсы нысан болуы мүмкін. Мысалы тәуекелдерді беру ресурстардың бағаланған құнына және тиісті тәуекелдерге өлшеулі сомаға сақтандыру көмегімен, сондай-ақ ұйымның бизнес-операциялары үшін ресурстардың маңыздылығын ескере отырып, жүзеге асырылуы мүмкін.

Егер олар тиісті түрде осы тәрізді жұмыстарды орындау үшін жарақтандырылған болса, сындарлы маңызды бизнес-ресурстармен немесе үшінші тараптардың процестерімен немесе аутсорсингтік серіктестермен жұмыс істеу үшін пайдалануда тағы бір мүмкіндік бар. Бұл жағдайда тиісті шартқа қажетті қауіпсіздікті қамтамасыз етуді кепілдендіретін, барлық қауіпсіздік талаптары, басқару мақсаттары мен басқару құралдары қосылу үшін қамқорлық жасау қажет. Бұл ретте көптеген жағдайларда аутсорсингке ақпараттарды берудің және ақпараттарды өңдеу құралдарының қауіпсіздігі үшін түпкілікті жауапкершілік алғашқы ұйымдастыруда қалатынын ұмытпаған жөн.

Тәуекелге тартылған ресурстар осы АҚБЖ-ны қолдану аясынан шыққан жағдайы тәуекелдерді берудің тағы бір мысалы бола алады. Бұл жағдайда аса маңызды ақпаратты қамтамасыз ету барынша қарапайым және арзан болуы мүмкін, бірақ бизнес үшін қажетті барлық ресурстар интерфейс пен тәуелділік арқылы осы АҚБЖ-ға қосылуы үшін қамқорлық жасауы қажет.

5. 6-Кезеңнің нәтижесі:

Осы кезеңнің нәтижесінде 5.1 – 5.5 кезеңдерінде сипатталған процестердің көмегімен бағаланған барлық тәуекелдер үшін тәуекелдерді өңдеудің барынша келетін нысаны сәйкестендірілген және құжаттандырылған болуы тиіс.

5.7 Басқару қауіпсіздігінің құралдарын таңдау

5.7.1 Қауіпсіздікті басқару құралдарын таңдау туралы

Қаралып отырған АҚБЖ-ны қолдану аясы шеңберінде бағаланған тәуекелдерді азайту үшін қауіпсіздікті басқарудың қажетті және негіздемелі құралдарын сәйкестендірілген және таңдау қажет. Басқару құралдары *ҚР СТ ИСО/МЭК* 17799 стандартынан немесе *ҚР СТ ИСО/МЭК 27*001 стандартынан, А-қосымшасынан, сондай-ақ қосымша көздерден таңдап алынуы мүмкін. Басқару құралдарының таңдау мақсаты осы ұйым үшін оңтайлы деңгейге дейін тәуекелдерді азайту болып табылады. Бұл таңдау

тәуекелдерді бағалау нәтижесінде негізделуі тиіс, мысалы, осалдық тиісті қауіптермен бірге қай жерде қорғау қажет болады және оны қандай нысанда іске асырған жөн екендігін көрсетеді. Тәуекелдерді бағалау байланысын басқару құралдарын таңдауды (немесе қарама қарсы шешім) негіздеу үшін құжаттау керек.

Басқарудың іске асырылған қаражаты оларды тиімділіктің жеткіліксіздігі жағдайында алып тастау немесе жетілдіру ниетімен сүйемелдеуді қоса алғанда шығындарды салыстыру негізінде қайта бағалауға тартуы тиіс. Бұл жерде басқарудың сәйкес келмейтін құралдарын кейбір кезде алып тастау оған басқарудың басқа құралдарын қосу мүмкіндігімен оны орнына тастап кетуден қарағанда барынша жоғары тұратындығын атаған жөн. Егер тәуекелдердің бағалауы орындалған болса, онда бұл процесс ЖІБТ моделінде «бағалау» кезегінің нәтижелерін қосуы тиіс.

Іске асыру үшін басқару құралдарын таңдаған кезде көптеген факторларды қараған жөн, оның ішінде:

– Басқару құралдарды пайдаланудың жеңілдігі,

– Пайдаланушы үшін ашықтық,

– Пайдаланушыға олардың функциясының орындау үшін берілетін көмек,

– Басқару құралдарының салыстырмалы қуаттылығы,

– Орындалатын қызметтердің үлгілері – алдын алу, ұстап қалу, тауып алу, қалпына келтіру, түзету, жөндеу, мониторинг және хабарлау.

Әдетте басқару құралдары бірнеше санамалаған функцияларды бірден орындайды және ол көп функция орындаса, соншалықты жақсы болмақ. Жалпы қауіпсіздікті немесе басқару құралдарын іске асырудың жиынтықтығын тексеру кезінде, егер бұл жалпы мүмкін болса, функциялардың аталған үлгілерінің арасындағы теңгерімді сақтаған жөн. Бұл шара жалпы қауіпсіздікті барынша тиімді және оңтайлы қамтамасыз етуді іске асыруға көмектеседі. Бұған қоса басқару құралдарын таңдаған кезде бірін бірі қолдайтын және толықтыратын басқарудың операциялық (техникалық емес) және техникалық құралдарының арасындағы теңгерімді ескерген жөн. Операциялық жүйелерге физикалық, кадрлық және әкімшілік қауіпсіздікті қамтамасыз ететіндер жатады.

Басқару құралдарын таңдаған кезде тәуекелдерді азайтудың аса маңызды факторынан басқа, сондай-ақ құндылық факторын орындаған жөн. (сондай-ақ 5.7.2 бөлігінің төменгі жағын қараңыз). Іске асырылуы мен қолдауы қауіпсіздікті қамтамасыз етуге бөлінген, алдыңғы жолы келісілген бюджетке қарағанда қымбатқа түсетін басқару құралдарын ұсыну орынсыз болмақ, сондықтан неғұрлым арзан балама нұсқаларын тапқан орынды. Алайда егер осы тәрізді бюджет іске асыру үшін таңдап алынған. Басқару құралдарының санын немесе сапасын азайтуға алып келсе, бұл

тәуекелдердің қаламаған қабылдауына алып келуі мүмкін болғандықтан, өте сақ болған жөн. Басқару құралдарына арналған бекітілген бюджетті шектеулі фактор ретінде тек қана абайлап пайдалану қажет.

А-қосымшасында мысалда аталған қауіптер санына сәйкес, *ҚР СТ ИСО/МЭК* 17799 стандартынан басқарудың нақты құралдардың мысалдары келтірілген.

5.7.2 Тәуекелдерді азайту мен қабылдау

5.6-бөлімінде «тәуекелдің азаюы» нұсқасы таңдап алынған барлық тәуекелдер үшін тәуекелдерді оңтайлы ретінде белгіленген деңгейге дейін төмендетуге мүмкіндік беретін басқарудың қажетті құралдарын таңдау керек. Басқару құралдарын сәйкестендіру үшін осы тәуекелдерге байланысты қауіпсіздік талаптарын (яғни қауіптер мен осалдықтар, құқықтық және бизнес-талаптар) және тәуекелдерді бағалаудың қалған барлық нәтижелерін қараған пайдалы. Басқару құралдары бағалаған тәуекелдерді бірнеше әртүрлі тәсілдермен азайтуға мүмкіндік береді, мысалы:

– Осы тәуекелге алып келетін қауіптің ықтималдылығын немесе осалдық ықтималдылығын азайта отырып;

– Құқықтық талаптар мен бизнес-талаптарды орындауды қамтамасыз ете отырып;

– Тәуекелдер туындаған жағдайда мүмкін болатын әсерлерді азайта отырып;

– Оларға ден қоя отырып және қалпына келтіруді орындай отырып, қаламаған оқиғаларды тауып алу арқылы.

Ұйымның осы АҚБЖ-ның ішінде өз ресурстарын қорғауды қамтамасыз ету үшін санамаланған тәсілдердің (немесе олардың үйлесімінен) ішінен біреуін таңдауы бизнес шешім болып табылады және ұйым жұмыс істеуге тура келетін бизнестің шарттары мен міндеттемесіне байланысты болмақ. Басқару құралдарының, ұйымның нақты қажеттіліктері мен және қабылданған шешімді негіздеуіне сәйкестікті сақтаған әрқашан маңызды.

Сәйкес келетін, тәуекелдерді оңтайлы деңгейге дейін азайтуға мүмкіндік беретін басқару құралдарды сәйкестендіруден кейін осы басқару құралдары нақ қай деңгейде екенін бағалау қажет, оларды іске асырған жағдайда тәуекелдерді азайту – бұл азайтылған тәуекел қалдық тәуекел деп аталады. Әдетте осы бір қалдық тәуекелді бағалау қиынға соғады, бірақ басқару құралдары қаншалықты тиісті қауіпсіздік талаптарын бағалау деңгейін азайта алатындығына баға қойған орынды – бұл қорғауды қамтамасыз етуді жеткілікті деңгейде кепілдендіруге мүмкіндік береді.

Егер қалдық тәуекел оңтайлы болмайтын болса, бұдан әрі не істеу керектігі туралы шешім қабылдау қажет. Мүмкін нысандардың біреуі

түбінде осы тәуекелді оңтайлы деңгейге дейін азайту үшін қосымша басқару құралдарын дайындау болып табылады. Әдетте оңтайлы емес тәуекелдерді қалдыруға жол бермеу ұсынылса да, барлық тәуекелдерді оңтайлы деңгейге дейін азайту барлық жағдайда немесе қаржылық көзқарасынан алғанда жүзеге асырылмауы мүмкін.

Таңдап алынған басқару құралдарын іске асырғаннан кейін тәуекелдер кез келген жағдайда қалып қояды. Ұйымның ақпараттық жүйелері абсолютті қауіпсіздік етуге болмайды. Осының салдарынан іске асырылған басқару құралдарының қаншалықты жақты жұмыс істейтіндігін түпкілікті бағалау үшін басқару құралдарының (қақтығыстар немесе журналдардың файлдары туралы есептер сияқты) әрекетін іске асыру мен нәтижелерін тексеру қажет. Бұл әрекеттер ЖІБТ моделіндегі «бағалау» кезеңінің бір бөлігі болып табылады және бұдан кейін сәйкестендірілген жетілдіру қауіпсіздікті барынша тиімді қамтамасыз ету үшін «түзету» кезеңінде іске асырылуы тиіс.

5.6-кезеңінің нәтижесі:

Осы кезеңнің нәтижесінде осы нұсқаның көмегімен өңдеу үшін 5.6 кезеңінде сәйкестендірілген барлық тәуекелдерді азайтуға мүмкіндік беретін басқарудың құралдары таңдап алынуы тиіс.

6 Тәуекелдерді бағалауға арналған тәсілдер

6.1 Кіріспе

5 бөлімде тәуекелдерді жалпы бағалаудың процестерін сипаттау келтіріледі. 5 бөлімде айтылғандай тәуекелдерді бағалауға қажетті тәсілді ұйымның өзі таңдауы қажет, сондықтан осы бөлімде тәуекелдерді бағалауға тәсілі үшін әртүрлі нұсқалар сипатталады. Осы бір әртүрлі тәсілдер талап етілетін уақыт саны мен жұмыс көлемімен, сондай-ақ бөлшектердің талдауының тереңдігімен ерекшеленеді. Ұйымның тәуекелдерді бағалауға тәсілді өзі таңдай алатындығына қарамастан, ұйымның бизнес талаптары мен қауіпсіздік талаптарын орындауды қамтамасыз ету үшін тәуекелдерді бағалаудың қолданылатын тәсілі (тәсілдері) жеткілікті шарада барабар және толық болып табылатындығын кепілдендіру қажет.

Егер, мысалға, ұйым немесе АҚБЖ және оның ресурстары төмен және орта деңгейден жоғары емес бизнес талаптарға ие болса, онда Тәуекелдерді базистік бағалау (Basic Risk Assessment) (6.2 қараңыз) тәсілі жеткілікті болуы мүмкін. Егер қауіпсіздік талаптары барынша толық және арнайы бағаларды талап ететін неғұрлым жоғары деңгейде болса , онда Тәуекелдерді бөлшектеп бағалау (Detailed Risk Assessment) (6.3 және 6.4 қараңыз) тәсілі талап етілуі мүмкін. Кез келген жағдайда таңдап алынған тәсіл *ҚР СТ ИСО/МЭК* 27001 стандартында келтірілген барлық өлшемдерге сәйкес келетінін кепілдендіру қажет, әсіресе:

– Ресурстарды сәйкестендіру (5.1 тармағын қараңыз);

– Қауіптер мен осалдықтарды, сондай-ақ барлық басқа қажетті қауіпсіздік талаптарын сәйкестендіру (сондай-ақ 5.3 тармағын қараңыз);

– Ресурстардың құпиялылығын, толықтықты мен қол жетімділігін жоғалтуы мүмкін ықпал етулерді сәйкестендіру (сондай-ақ 5.2 тармағын қараңыз);

– Жоғарыда санамаланған ақпараттар негізінде зиянды және тәуекелдердің туындау ықтималдылығын бағалау, сондай-ақ тәуекелдер деңгейін бағалау (сондай-ақ 5.4 және 5.5 тармақтарын қараңыз);

– Тәуекелдерді өңдеудің барынша сәйкес келетін нұсқасын сәйкестендіру (сондай-ақ 5.6 тармағын қараңыз);

– Тәуекелдерді оңтайлы деңгейге дейін азайту үшін басқару мақсаттары мен басқару құралдарын таңдау (сондай-ақ 5.7 тармағын қараңыз).

6.2 Тәуекелдегі базистік бағалау

Базистік тәсіл 5-бөлімде сипатталған процестерді тура және тікелей қолдану негізінде қауіпсіздікті басқару құралдарының жиынтықты таңдауын ұйғарады.

Бұл тәсіл ұйымның негізгі және маңызды қажеттіліктері мен талаптарын сәйкестендіру және бағалау негізінде қорғаудың базистік деңгейіне қол жеткізе отырып, ұйымға өзінің АҚБЖ әзірлеуіне мүмкіндік береді. Қорғаудың базистік деңгейі тәсілді осындай тікелей және қарапайым жолдардың көмегімен қол жеткізген, қауіпсіздік талаптарының төмен деңгейі бар қандай да бір ұйымның бөлігі үшін немесе кейбір жағдайларда – тіпті барлық ұйым үшін егер оның қауіпсіздік талаптарында қауіпсіздік талаптарының жеткілікті төменгі деңгейі бар болса сәйкес келуі мүмкін. Бірақ кез келген ұйым үшін *ҚР СТ ИСО/МЭК 27001* стандарты бойынша сертификациялау кезінде егер дәл ол таңдап алынса, базистік тәсілдің жеткіліктілігін негізде алуы маңызды.

Осы тәсілді қолданудың үлгілік мысалы мүлдем қиын бизнес операциялар жүргізілмейтін және ақпараттарды өңдеу, желілерде жұмыс істеу өте үлкен емес ұйымның бір бөлігі болып табылуы мүмкін. Бұл тәсіл кейбір шағын ұйымдарда да қолданылуы мүмкін. Алайда неғұрлым күрделі бизнес ортасы бар, ақпараттық жүйелерге негізделген технологияларды кеңінен пайдалануға байланысты болатын және коммерциялық маңызды ақпараттарды өңдеуге қатысатын шағын ұйымдар да болуы мүмкін.

ҚР СТ ИСО/МЭК 27001 стандартының контекстінде осы тәсіл ақпараттар мен қаралатын ресурстар, іске асыруға жататын басқару мақсаттарын сәйкестендіру және осы мақсаттарды қанағаттандыратын басқару құралдарын бұдан кейінгі таңдау үшін ұйымның бизнес-талаптарын жүйелік бағалауды міндетті түрде қамтиды (5.3 және 5.4 бөлімін қараңыз).

Базистік бағалау тәсілі 5 бөлімде сипатталған процестерге негізделген мынадай әрекеттерді қамтиды және барлық көздердің ішінен қауіпсіздік талаптарын есепке алынуы тиіс.

Тәуекелдерді бағалау мен тәуекелдерді басқару міндеттері	**Орындау кезіндегі әрекеттер Тәуекелдерді сервистік бағалау**
Ресурстарды сәйкестендіру мен бағалау (5.1 және 5.2)	АҚБЖ-ны қолдану аясының шеңберінде бағаланатын осы бизнес-ортамен, операциялармен және ақпараттармен байланысты ресурстардың тізімін құрастыру және .бағалаудың қарапайым шәкілін пайдалана отырып, олардың маңыздылығының деңгейін анықтау
Қауіпсіздік талаптарын сәйкестендіру мен бағалау (5.3 және 5.4)	Қауіпсіздік талаптарын сәйкестендіру (бұл ретте жалпыланған немесе кеңінен танымал қауіптер мен осалдықтардың бақылау тізімін пайдалануға болады) және бағалаудың қарапайым шәкілін пайдалана отырып, барлық сәйкестендірілген қауіпсіздік талаптарының деңгейін айқындау
Тәуекелдердің есебі (5.5)	Ресурстар мен қауіпсіздік талаптар туралы ақпараттардың негізінде есептің қарапайым кестесін пайдалана отырып тәуекелдерді есептеу
Тәуекелдерді өңдеу нұсқаларын сәйкестендіру және бағалау (5.6)	Сәйкестендірілген тәуекелдердің ішінен әрқайсысы үшін тәуекелдерді өңдеудің тиісті нұсқасын сәйкестендіру; тәуекелдерді өңдеу жоспары үшін нәтижелерді құжаттандыру
Қауіпсіздікті басқару құралдарын таңдау, тәуекелдерді азайту мен қабылдау (5.7)	Сәйкестендірілген ресурстардың әрқайсысы үшін *ҚР СТ ИСО/МЭК* 17799:2005 стандартының ішінен мәнді болып табылатын басқару мақсаттары мен басқару құралдарын сәйкестендіру. Таңдап алынған басқару мақсаттары мен басқару құралдары тәуекелдерді оңтайлы деңгейге дейін азайтатындығын кепілдендіру

Жалпыланған немесе кеңінен танымал қауіптер мен осалдықтардың тізімін пайдалану бағалау бойынша әрекеттерден кейін және талдау процесінің жіберуге және бағдарлауға көмектесу мүмкін. Осы базистік тәсіл мен басқару құралдарын тиісті талдау туралы барынша толық ақпарат [4] келтірілген.

Бұл тәсіл Б қосымшасында сипатталған кестелік әдістің оңайлатылған нұсқасының көмегімен қолданылуы мүмкін (Б.2.2 қараңыз). Бұндай тәсіл кезінде, мысалы, қауіпсіздік талаптарының екі деңгейі (мысалы, жоғары

және төмен) және алдында белгіленген шәкіл бойынша ресурстарды бағалау (мысалы, жоғары деңгей, орта деңгей және төменгі деңгей) пайдаланылуы мүмкін.

Төмендегі кестеде келтірілген сандар тәуекелдің деңгейін көрсетеді (мысалы, 0-ден 4-ке дейін).

	Қауіпсіздік талаптарының деңгейі	**Төменгі**	**Жоғары**
Ресурстардың мәнділігінің бағасы	Төменгі деңгей	0	2
	Орта деңгей	1	3
	Жоғары деңгей	2	4

Тәуекелдердің осы кезеңдерін қандай тәуекелдерді бірінші өңдеу қажет және қайсына көбірек назар аударған жөн, сондай-ақ тәуекелдерді өңдеудің таңдау нұсқаларын пайдалану мүмкін екенін шешу үшін пайдалануға болады. Тәуекелдердің азайту нұсқасы таңдап алынған тәуекелдер үшін қаралатын АҚБЖ үшін тиісті бизнес талаптар мен қауіпсіздік талаптарына сәйкес келетін тәуекелдердің оңтайлы деңгейін сәйкестендіру қажет. Жоғарғы кестеде келтірілген мысалдар үшін тәуекелдің оңтайлы деңгейін 2-ден жоғары таңдамау ұсынылады.

Тәуекелдерді базистік бағалау тәсілі мынадай бірқатар артықшылықтарға ие:

– Тәуекелдерді бағалау үшін ең аз ресурстар талап етіледі, басқару құралдарын таңдау үшін қажетті уақыт шығыны және жұмыс көлемі азаяды. Әдетте басқарудың қажетті құралдарын сәйкестендіру үшін айтарлықтай ресурстар талап етілмейді,

– Басқарудың сәйкес немесе ұқсас құралдары бірнеше ресурстар үшін жеңіл бейімделген болуы мүмкін. Егер ұйым ресурстарының көпшілігі жалпы ортада жұмыс істесе және егер бизнес талаптары мен қауіпсіздік талаптары ұқсас болып табылса онда осы басқару құралдары экономикалық тиімді шешімдерді қамтамасыз етуі мүмкін.

– Осы тәсіл мынадай жетіспеушіліктерге ие:

– Егер қауіпсіздік деңгейі өте жоғары болып табылса кейбір ресурстар үшін мүлдем қымбат тұратын немесе басқарудың артық шектеулі құралдары таңдап алынуы мүмкін, ал егер бұл деңгей төмен болып табылса іске асырылған қауіпсіздік кейбір ресурстар үшін жеткіліксіз болуы мүмкін.

– Өзгерістердің қауіпсіздігі үшін маңызды басқаруда қиындықтар туындауы мүмкін (бұл ЖІБТ моделіндегі «Бағалау» және «Түзету» кезеңдерінде талап етіледі). Мысалы, егер АҚБЖ-ның өн бойында өзгерістер

болатын болса, жаңа жағдайда басқарудың алғашқы құралдары жеткілікті ме екенін бағалау қиын болуы мүмкін.

6.3 Тәуекелдерді бөлшектеп бағалау

Басқару құралдарын таңдау ресурстар ұшырайтын сәйкестендірілген тәуекелдерге негізделеді және ол тәуекелдердің қолайлы деңгейге дейін (егер қатерді өңдеудің осы нұсқасы таңдалынса) төмендеуі қамтамасыз етіледі.

Тәуекелдерді егжей-тегжейлі бағалау өте ресурстарды қажет ететін процес болуы мүмкін, сондықтан бизнес ортаның шекарасын, операцияларды, ақпараттарды және бағаланатын АҚБЖ-ны қолдану саласындағы ресурстарды мұқият айқындау қажет болады. Бұдан өзге бұндай әдіс басшылық тарапынан қатты назар аударуды қажет етеді.

Бағаланған қатерлерге сәйкес басқару құралдары қол жеткізілуі тиіс басқару мақсаттарына байланысты *ҚР СТ ИСО/МЭК* 17799 стандартынан таңдап алынуы мүмкін. Бұл жалпы әдіс 6.2 –бөлімінде сипатталған тәуекелді базистік бағалау әдісінен ерекшеленеді, онда ресурстарды және қауіпсіздік талаптары 5-бөлімде сипатталған принциптерде егжей-тегжейлі талдау орындалады. Тәуекелдерді әр түрлі бағалау немесе есептеуге қатысты Б-қосымшасында келтірілген ұқсас әдістердің бірі қолданылады.

Тәуекелдерді бағалау міндеттер және тәуекелдерді басқару	**Тәуекелдерді егжей-тегжейлі бағалауды орындау кезіндегі әрекеттер**
Ресурстарды сәйкестендіру және бағалау (5.1 және 5.2)	Осы АҚБЖ-ны қолдану саласы шегінде бизнес ортамен, операциялармен және ақпараттармен байланысты барлық ресурстардың тізімін сәйкестендіру және жасақтау, әрбір ресурс үшін бағалау шәкілін беру, осы шәкіл бойынша бағалауды айқындау (әрбір: құпиялылық, тұтастық және қол жетімділік факторы үшін сондай-ақ қажет болған кезде басқа да факторлар бойынша бір бағалау
Қауіпсіздік талаптарын сәйкестендіру (5.3)	АҚБЖ-ны қолдану саласындағы ресурстардың тізіліміне байланысты қауіпсіздіктің барлық талаптарын (қауіп-қатерлер мен әлсіздіктер, құқықтық талаптар және бизнес-талаптар) сәйкестендіру
Қауіпсіздік талаптарын бағалау (5.4)	Қауіпсіздік талаптары үшін қажетті бағалау шәкілін сәйкестендіру және әрбір сәйкестендірілген қауіпсіздік талабы үшін тиісті бағалауды айқындау

Тәуекелдерді есептеу (5.5)	Мысалы, Б қосымшасында келтірілген тәуекелдерді бағалау әдістерінің бірі немесе қандай да бір басқа түрі немесе қарастырылатын АҚБЖ қауіпсіздігінің талаптарына сәйкес келетін ұқсас әдістің көмегімен тәуекелдерді есептеу (ресурстар мен қауіпсіздік талаптарын, сондай-ақ жоғарыда көрсетілген бағалау нәтижесінде алынған олардың бағалау деңгейлерін ескере отырып)
Тәуекелдерді өңдеу нұсқаларын сәйкестендіру және бағалау (5.6)	Әрбір сәйкестендірілген тәуекелдер үшін тәуекелдерді өңдеу жөніндегі ыңғайлы әрекеттерді сәйкестендіру. Сәйкестендірілген нұсқаның нақтылығын, оның барабарлығын және барлық бизнес-талаптар мен қауіпсіздік талаптарына сәйкестігін бағалау. Тәуекелдерді бағалау жоспары үшін нәтижелерді құжаттау
Қауіпсіздікті басқару құралдарын таңдау, тәуекелдерді азайту және таңдау (5.7)	Тәуекелдерді бағалаудың таңдалған әдісі үшін тәуекелдің қолайлы деңгейін айқындау және қолайлы тәуекелдің бұл деңгейінің бизнес-талаптар мен қарастырылатын АҚБЖ қауіпсіздігінің талаптарына сәйкес келуі. Тәуекелдерді төмендету нұсқасынан таңдалған тәуекелдер үшін бұл тәуекелдерді қолайлы деңгейлерге дейін азайтуға мүмкіндік беретін басқару мақсаттарына және басқару құралдарына ыңғайлы *ҚР СТ ИСО/МЭК* 17799 стандартынан таңдау керек

Бұл әдістің басымдығы мынаны білдіреді:

– Ұйым қауіпсіздігінің ресурстарға және АҚБЖ талаптарын көрсететін қауіпсіздіктің деңгейін сәйкестендіруге мүмкіндік беретін қауіпсіздік қатерлері туралы дәл және егжей-тегжейлі ұғымға қол жеткізіледі,

– Қауіпсіздігі үшін маңызды өзгерістерді басқару кезінде («Бағалау» ж»не ЖІБТ моделдерін «Түзету» кезеңдерінде қажет болатын) тәуекелдерді егжей-тегжейлі бағалау нәтижесінде алынған қосымша ақпаратты пайдалануға болады

– Бұл әдістің мынадай кемшілігі бар:

– Сапалы нәтижелерді алу үшін көп уақыт, жұмыстың ауқымды көлемі және жоғары біліктілігі қажет болады.

6.4 Аралас әдіс

Бұл әдіс тәуекелдің әлеуетті жоғары деңгейін және бизнес операциялар үшін сындарлы болып табылатын АҚБЖ-ны қолдану саласынан алынған сол ресурстар үшін сәйкестендіруді ұсынады. Бұл нәтижелердің негізінде

АҚБЖ-ны қолдану саласына кіретін барлық ресурстар тиісті қорғауға қол жеткізу үшін басқа ресурстарға бөлінеді. Тәуекелдерді (6.3-т. қараңыз) және ресурстарды егжей-тегжейлі бағалау тәуекелдерді базистік бағалау әдісі үшін қажет. Бұндай әдіс жоғарыда сипатталған 6.2 және 6.3 тармақтары әдістерінің басымдықтарын біріктіруге мүмкіндік береді. Осының салдарынан ол басқару құралдарын сәйкестендіруге кететін уақыт пен күшті азайтуға және бұл ретте ұйымның ресурстарын тиісті бағалау мен қорғауды қамтамасыз ететін ойдағыдай ымыра болып табылады.

Екі әдістің басымдықтарын біріктіруден басқа бұл әдіс мына басымдыққа ие:

– қаражат пен ақша барынша пайдалы болатын тұста қолданылуы мүмкін, тәуекелдердің жоғары деңгейі бар ұйымның ақпараттық жүйелері бірінші кезекте ескерілуі мүмкін.

– Бұл әдістің мынадай кемшілігі бар:

– тәуекелдердің жоғары деңгейі бар ақпараттық жүйелер бұрыс сәйкестендірілген жағдайда бұл әдіс қате нәтижелерге әкелуі мүмкін, яғни тәуекелдерді егжей-тегжейлі бағалау қажет болатын жүйелерге тек тәуекелдерді Базистік бағалау әдісі ыңғайлы болады.

6.5 Тәуекелдерді бағалауға /тәуекелдерді басқаруға қажетті әдісті таңдау

6.5.1 Таңдауға әсер ететін факторлар

Осы бөлімнің алдыңғы тармақтарында айтылғандай ұйымның тәуекелдерін бағалау үшін барлық ұйымда қолданылатын әр түрлі жалпы әдістерді таңдап алуға болады. Жоғарыдағы тармақтарда мұндай әдістердің басымдықтар мен қателіктері көрсетілді. Ұйымда дәл қандай әдісті таңдау бірнеше факторларға байланысты болады, оның ішінде:

– олардың бизнес ортасы мен бизнес қызметінің түрі;

– бизнесті ұстайтын ақпарат пен қосымшаларды өңдеуге тәуелділік;

– бизнес-жүйелердің және ұстаушы жүйелердің қосымшалар мен сервистердің күрделілігі;

– әріптес компаниялардың саны мен сыртқы іскери және шарттық қатынастардың көлемі.

Бұл факторлар әдетте қызметтің барлық бағыттары үшін жалпы болуы тиіс, сондықтан барлық ұйым үшін тиісті әдісті таңдауы кезінде бұл факторларды әдістердің басымдықтарымен және кемшіліктерімен қатар ескеру керек. Әдісті таңдау туралы шешімді *ҚР СТ ИСО/МЭК 27001* стандартында белгіленген (6.1-т. қараңыз) өлшемдерді сақтау кезінде ұйымның өзі қабылдауы тиіс. Тәжірибеде мына ережелерді ұстау

ұсынылады: ұйым және оның бизнесі үшін қауіпсіздік қаншалықты маңызды және қажетті болса, қауіпсіздікті қамтамасыз етуге соншалықты уақыт пен қаражатты жұмсау керек.

6.5.2 *ҚР СТ ИСО/МЭК 27001* стандарты бойынша АҚБЖ-ны сертификаттау

ҚР СТ ИСО/МЭК 27001 стандарты бойынша ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) сертификаттау үшін тәуекелдерге тиісті бағалау жүргізу туралы талаптарды орындау және бұл бағалаудың нәтижелерін қолданушылық туралы ережелерде (2-бөлімді қараңыз) құжаттау қажет болады. Бұл шарт сертификаттау процесінің маңызды бөлігі болып табылады. Сондықтан ұйым тәуекелдерді бағалаудың барынша барабар әдісін таңдауы өте маңызды.

6.6 Шағын және орта кәсіпорындарда тәуекелдерді бағалау

Шағын және орта кәсіпорындар үшін пайдалы болатын тәуекелдерді бағалаудың әдістерінің жалпы ережесі жоқ, өйткені бұл шешім бизнес-талаптарға және қауіпсіздік талаптарына негізделуі тиіс, әрі ұйымның мөлшеріне қатысты бола бермейді. Төменде 6.5.1-тармағында көрсетілген факторларға олардың қалайша қатысты болатыны туралы жалпы ұғымдарға негізделген шағын және орта кәсіпорындар үшін бірнеше ескертпелер келтіріледі.

Бизнес операциялардың күрделілігі қаншалықты аз болса, жүйелері де соншалықты аз, оның үстіне ақпараттық қауіпсіздік талаптары да қарапайым болуы мүмкін және шағын әрі орта кәсіпорындардың басым бөлігі үшін бұл мүлтіксіз факт болып қала береді; алайда бизнес талаптары өте күрделі шағын және орта кәсіпорындары да бар. Шағын және орта бизнес кәсіпорындары көптеген ұйымдар үшін жеткізуші болуы мүмкін және *ҚР СТ ИСО/МЭК* 17799 стандартынан басқару құралдарының бірқатарларын өткізу туралы шарт жасалуы мүмкін. Мысалы, мұндай кәсіпорын *ҚР СТ ИСО/МЭК* 17799 стандартының «Сырт ұйымдардың ену қауіпсіздігі» аспектілерін ескеріп, сондай-ақ «Деректермен және бағдарламалармен алмасу туралы келісім» бөлімінің, «Компьютерлік қосымшаларға енуді басқару» бөлімдерінің және «Ақпараттық жүйелерді әзірлеу және сүйемелдеу» бөлімнің аспектілерін қолдану қажеттілігі мәселесін қарауы тиіс. Одан өзге «Ресми талаптарға сәйкестік» бөлімінің қандай аспектілерін қолдану қажеттілігін айқындау керек болады.

Кәсіпорынның ақпаратты өңдеуге және есептеу жүйелерін пайдалануға тәуелділігі тым жоғары болуы мүмкін және олардың бизнесі айтарлықтай шамада осындай жүйелерді пайдаланумен айқындалады. Мысалы шағын және орта кәсіпорындар зияткерлік меншік терминдері бойынша мазмұны мен дизайнының нарықтық құны жоғары ойын-сауық индустриясына

арналған ақпараттық өнімдерді өндіру үшін осы жүйелерді қолдануы мүмкін.

Шағын және орта кәсіпорындар қауіпсіздіктің талаптарын және тапсырушының талаптарын қанағаттандыратын үш әдістің (6.2, 6.3 және 6.4 бөлімдерін қараңыз) біріне және қауіпсіздікті басқару құралдарын іске асыруға сәйкес қатерлерді бағалауға жұмсалатын қаражат арасындағы теңгерімді табуы тиіс. Орта және шағын кәсіпорындарға олардың бизнесі қандай болғанына қарамастан қауіпсіздікті басқарудың кейбір құралдарына және тәуекелдерді Базистік бағалаудың әдістерін іске асыруы қажет, бұлар басқару құралдарының қайсысы тиімді екенін айқындауға мүмкіндік береді. Әрине қауіпсіздік саясатын қандай да бір нысанда іске асыру, енуді бақылаудың кейбір құралдарын орнату және құқықтық әрі нормативтік талаптарды сақтау қажет болады. Бұдан өзге 6.3. бөлімінде сипатталған қатерлерді егжей-тегжейлі бағалау әдісінің көмегімен іскерлік қатынастар нәтижесінде туындайтын кейбір нақты талаптарды арнайы қарау қажет болады.

А қосымшасы
(анықтамалық)
Қауіптер мен осалдықтар мысалдары

Төменде көрсетілген тізімдер *ҚР СТ ИСО/МЭК* 17799 стандартында көрсетілген басқару және басқару құралдарының мақсаттары мен байланысты қатерлер мен осалдықтардың бірнеше мысалдарын қамтиды. Бұл қатерлер мен осалдықтардың тізімі түпкілікті болып табылмайды және оларды *ҚР СТ ИСО/МЭК* 17799 стандартында келтірілген басқару құралдары мен байланысты ұғымдарды білдіретін мысалдар ретінде ғана қарастыру керек.

Бұл жағдайда тиісті түрде ескеретін және бизнес орта үшін маңызды қатерлер мен осалдықтардың толық ауқымын сәйкестендіретін тәуекелдерді бағалауға және басқаруға арналған әдістерді ұйымға қабылдау қажеттігін білдіреді.

А.1 Қатерлер тізімінің мысалы

Төменде [3] алынған тізімдер келтіріледі Бұл тізім мұнда иллюстрация үшін келтірілген сондықтан толық және түпкілікті ретінде қаралмауы тиіс.

Аэрозолдің/шаңның бөлігі	Аппараттық ақаулар
Желдету жүйесіндегі бұзушылық	Дауыл
Террорлық акт	Бағдарламалық қамтамасыз етудің заңсыз импорты/экспорты
Байланыс жүйесіне заңсыз ену	Бағдарламалық қамтамасыз етуді заңсыз пайдалану
Байланыс желісінің /кабелінің бүлінуі	Ереуіл
Ақпараттарды тасушылардың бұзылуы	Найзағайдың түсуі
Жерсілкінісі	Техникалық қызмет көрсетудің қателігі
Тыңдау	Зиян әкелетін бағдарламалық қамтамасыз ету (мысалы, вирустар, желілік зақымдағыштар, троян аты)
Қоршаған ортаны ластау (және табиғи немесе антропогендік апаттардың басқа да нысандары)	Пайдаланушының сәйкестендіру ақпаратын ауыстыру
Температура мен ылғалдылықтың экстремалдық мәні	Хабарлардың дұрыс бағдарландырылмауы немесе қайта бағдарландырылмауы
Байланыс сервисінің бас тартуы	Авторизацияланбаған пайдаланушылардың желілік қолжетімділігі

Желі компоненттерінің ақаулары	Ресурстарды дұрыс пайдаланбау
Қоректендіру жүйесіндегі бас тарту	Жедел қолдау персоналының қатесі
Су құбырының апаты	Қоректендіру бойынша лақтырулар
Өрт	Бас тартудың мүмкіндіктері (мысалы, қызметтен, транзакциядан, хабарларды алу/жіберу
Су тасқыны	Бағдарламалық қамтамасыз етудің ақауы
Персоналдың жетіспеушілігі	Дерек тасығыштарды заңсыз пайдалану
Ұрлық	Байланыс құралдарын заңсыз түрде пайдалану
Трафикті талдау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдалану
Трафикті қайта жүктеу	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Деректерді беру қатесі	Пайдаланушының қатесі
Бағдарламалық қамтамасыз етуді заңсыз пайдалану	Зиянды қасақана келтіру

Қауіптің типіне қатысты оның жүзеге асырылуы мынадай түрлі салдарларға әкеп соғуы мүмкін:

Есептеуіш ортада деректер мен бағдарламалық қамтамасыз етуді бірлесіп пайдалануда қамтамасыз ететін кездейсоқ және қасақана құралдары	Техникалық нұсқауларды сақтамау нәтижесіндегі қауіпсіздіктерді бұзушылық
Дәл емес, толық емес немесе сәйкес келмейтін техникалық немесе лауазымдық нұсауқлықтардың немесе осы рәсімдердің жеткіліксіз жаңартылуы салдарынан қауіпсіздіктің бұзылуы.	
Қақтығыстарды өңдеудің рәсімдерін сақтамау нәтижесінде қауіпсіздіктердің бұзылуы.	Мердігер алаңындағы деректердің жоғалу ымырасы.
Үздіксіз жұмыстың дәл емес, толық емес немесе сәйкес келмейтін жоспарларын қамтамасыз ету, жеткіліксіз тестілеу немесе осы жоспарларды жеткіліксіз жаңарту салдарынан болған зиян	
Қызмет көрсетудегі, жүйелік ресурстарды беруден, ақпараттарды ұсынудағы бас тарту и	Пошталық бомбалар (Email bombs)
Себеп	Алаяқтық

Міндеттемелерді бөлу мен орындалмаған себепті қаражаттарды немқұрайлы немесе қасақана дұрыс пайдаланбау	Сындарлы және/немесе маңызды құралдар мен өңдеу құралдары ұсталатын алаңдардың/ғимараттардың/үй-жайлардың орналасқан жерін заңсыз ашу
Ақпараттарды заңсыз ашу	

А.2 Қауіптердің үлгілері және *ҚР СТ ИСО/МЭК* 17799 және *ҚР СТ ИСО/МЭК 27001* стандарттары

Төменде *ҚР СТ ИСО/МЭК* 17799 және *ҚР СТ ИСО/МЭК 27001* стандарттарында келтірілген басқару мақсаттарымен байланысты әртүрлі қатерлердің үлгісі төменде келтірілген.

А.2.1 Физикалық қауіпсіздік және жұмыс істеу ортасының қауіпсіздігі

Қорғалған салалар

Мақсат: Өндірістік үй-жайларға және ақпараттық сервистерге заңсыз физикалық енудің алдын алу, оларды бүлдіру және олардың жұмыс істеуіне қол сұғушылық.

Сындарлы немесе маңызды бизнес операциялардың ИТ-құралдары қорғалған салаларда орналастырылуы тиіс.

Өрт	Су тасқыны
Террористік акт	Дауыл
Жер сілкінісі	Көтерілістер
Қоршаған ортаны ластау (және табиғи немесе антропогендік апаттардың басқа нысандары)	Найзағайдың түсуі
Ұрлық	Қасақана зиян келтіру

Жабдықты қорғау

Мақсат: Ресурстардың жоғалуының, бүлінуінің немесе беделсіздендіру ресурстарының алдын алу, сондай-ақ ұйымның жұмысындағы үзілістер.

Қоршаған ортаға келтірілетін қауіптер мен қауіпсіздіктерді бұзу қатерінен жабдықты физикалық қорғауды қамтамасыз ету.

Аэрозолдың/шаңның бөліктері	Аппараттық ақау
Желдету жүйесіндегі бұзушылық	Техникалық қызмет көрсетудің қателігі
Байланыс сервисінің бас тартуы	Авторизацияланбаған пайдаланушылардың желілік қолжетімділігі
Желі компоненттерінің ақаулары	Ресурстарды дұрыс пайдаланбау
Қоректендіру жүйесіндегі бас тарту	Жедел қолдау персоналының қатесі
Су құбырының апаты	Қоректендіру бойынша лақтырулар
Өрт	Бас тартудың мүмкіндіктері (мысалы, қызметтен, транзакциядан, хабарларды алу/жіберу
Зиянды қасақана келтіру	

А.2.2 Компьютерлік жүйелері мен есептеу желілерін әкімшіліктендіру

Операциялық рәсімдер мен міндеттіліктер

Мақсат:Ақпаратты өңдеу үшін пайдаланылатын құралдардың дұрыс және сенімді жұмыс істеуін қамтамасыз ету.

Барлық компьютерлер мен желілердің жұмыс істеуін әкімшіліктендіру және қамтамасыз ету жөніндегі міндеттіліктер мен рәсімдерді айқындау қажет.

Өрт	Су тасқыны
Террористік акт	Дауыл
Жер сілкінісі	Көтерілістер
Қоршаған ортаны ластау (және табиғи немесе антропогендік апаттардың басқа нысандары)	Найзағайдың түсуі
Ұрлық	Қасақана зиян келтіру
Байланыс сервисінің бас тартуы	Авторизацияланбаған пайдаланушылардың желілік қолжетімділігі
Желі компоненттерінің ақаулары	Ресурстарды дұрыс пайдаланбау
Қоректендіру жүйесіндегі бас тарту	Жедел қолдау персоналының қатесі
Су құбырының апаты	Қоректендіру бойынша лақтырулар
Өрт	Бас тартудың мүмкіндіктері (мысалы, қызметтен, транзакциядан, хабарларды алу/жіберу
Осалдық	Су тасқыны
Террористік акт	Дауыл
Жер сілкінісі	Көтерілістер

А.2.3 Ұйымның тоқтаусыз жұмысын жоспарлау

Ұйымның тоқтаусыз жұмысын жоспарлаудың аспектілері

Мақсат: Ұйымның жұмыстағы үзілістеріне қарсы тұру және ірі апаттар мен зілзалалардың салдарларынан сындарлы өндірістік процестерді қорғауды қамтамасыз ету.

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар

А.2.4 Формалдық талаптарға сәйкес келу

Құқықтық талаптарды орындау

Мақсат: Заң күші бар қылмыстық және азаматтық заңнама міндеттемелерін, реттейтін немесе шарттық міндеттемелерді, сондай-ақ ақпараттық қауіпсіздіктерге талаптарды бұзудың алдын алу.

Ақпараттық жүйелерді әзірлеуге, сүйемелдеуге және пайдалануға қауіпсіздікке құқықтық және шарттық талаптар салынуы мүмкін.

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар

Ақпараттық жүйелердің қауіпсіздігін тексеру

Мақсат: Ұйымда қабылданған жүйелерге қауіпсіздік саясаты мен стандарттарына сәйкестікті қамтамасыз ету.

Ақпараттық жүйелердің қауіпсіздігін тұрақты түрде тексеру керек.

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар
Сәйкестендіру мен дәлме дәлдендіру тетігінің жоқ болуы	Қолданушының идентификациялық ақпараттарымен алмасу
Компьютерде жұмысты тоқтатқаннан кейін жүйеден шығу рәсімін пайдаланбау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы

Жүйелердің аудиті

Мақсат: Ақпараттық жүйелерге аудит процесінің бір жағынан әсер етуін және екінші жағынан аудит процесіне ақпараттық жүйелерді әсер етуін азайту.

Жұмыс жүйелерін және оларды тексеру уақытында аудит құралдарын қорғау үшін бақылау құралдары болуы қажет.

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану

Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар

А.3 Осалдықтар тізімінің үлгісі

Төменде келтірілген тізімдерде қауіпсіздіктің әртүрлі салаларындағы осалдықтың үлгілері, сондай-ақ бұл осалдықтарды пайдалануы мүмкін қатерлердің үлгілері келтірілген. Бұл тізімдер осалдықтарға бағалау жүргізу кезінде пайдалы болуы мүмкін.

Басқа да қатерлер де бұл осалдықтарды пайдалану мүмкін екендігін атап өту керек.

А.3.1 Персоналмен байланысты қауіпсіздік аспектілері (*ҚР СТ ИСО/МЭК* 17799)

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар
Сәйкестендіру мен дәлме дәлдендіру тетігінің жоқ болуы	Қолданушының идентификациялық ақпараттарымен алмасу
Компьютерде жұмысты тоқтатқаннан кейін жүйеден шығу рәсімін пайдаланбау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бағдарламалық қамтамасыз етуді тестілеудің болмауы немесе жеткіліксіздігі	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы

А.3.2 Физикалық қауіпсіздік және жұмыс істеу ортасының қауіпсіздігі (ИСО/МЭК 17799, 7-бөлім)

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар
Сәйкестендіру мен дәлме дәлдендіру тетігінің жоқ болуы	Қолданушының идентификациялық ақпараттарымен алмасу
Компьютерде жұмысты тоқтатқаннан кейін жүйеден шығу рәсімін пайдаланбау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бағдарламалық қамтамасыз етуді тестілеудің болмауы немесе жеткіліксіздігі	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Парольдерді қанағаттанарлықсыз басқару (жеңіл шешілетін парольдер, парольдерді сақтау, парольдерді жеткіліксіз тұрақты ауыстырмау)	Пайдаланушының сәйкестендірілген ақпараттарды ауыстырып қоюы
Әзірлеушілер үшін анық емес немесе толық емес ерекшеліктер	Бағдарламалық қамтамасыз етудегі ақаулар

А.3.3 Компьютерлік жүйелерді және есептеу желілерін әкімшіліктендіру (ИСО/МЭК 17799)

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі

Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар
Сәйкестендіру мен дәлме дәлдендіру тетігінің жоқ болуы	Қолданушының идентификациялық ақпараттарымен алмасу
Компьютерде жұмысты тоқтатқаннан кейін жүйеден шығу рәсімін пайдаланбау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бағдарламалық қамтамасыз етуді тестілеудің болмауы немесе жеткіліксіздігі	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Парольдерді қанағаттанарлықсыз басқару (жеңіл шешілетін парольдер, парольдерді сақтау, парольдерді жеткіліксіз тұрақты ауыстырмау)	Пайдаланушының сәйкестендірілген ақпараттарды ауыстырып қоюы
Әзірлеушілер үшін анық емес немесе толық емес ерекшеліктер	Бағдарламалық қамтамасыз етудегі ақаулар
Бақыланбайтын қайта жүктеу мен бағдарламалық қамтамасыз етуді пайдалану	Зиян келтіргіш бағдарламалық қамтамасыз ету
Парольдердің қорғалмаған кестесі	Пайдаланушының сәйкестендірілген ақпараттарды ауыстырып қоюы

А.3.4 Енуді басқару / Ақпараттық жүйелерді әзірлеу және сүйемелдеу (ИСО/МЭК 17799)

Осалдық	Осалдық қауіп арқылы қолданылады
Пайдаланушының күрделі интерфейсі	Жедел қолдау персоналының қателігі
Ақпараттарды тасығыштардың ақпараттарды тиісті түрде жоймай-ақ жоюы немесе қайта пайдалануы	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы

Бақылау журналының жоқ болуы	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану
Құжаттаманың жоқтығы	Жедел қолдау персоналының жоқ болуы
Өзгерістерге тиімді бақылаудың болмауы	Ақпаратты қамтамасыз етудегі ақаулар
Сәйкестендіру мен дәлме дәлдендіру тетігінің жоқ болуы	Қолданушының идентификациялық ақпараттарымен алмасу
Компьютерде жұмысты тоқтатқаннан кейін жүйеден шығу рәсімін пайдаланбау	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Бағдарламалық қамтамасыз етуді тестілеудің болмауы немесе жеткіліксіздігі	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Парольдерді қанағаттанарлықсыз басқару (жеңіл шешілетін парольдер, парольдерді сақтау, парольдерді жеткіліксіз тұрақты ауыстырмау)	Пайдаланушының сәйкестендірілген ақпараттарды ауыстырып қоюы
Әзірлеушілер үшін анық емес немесе толық емес ерекшеліктер	Бағдарламалық қамтамасыз етудегі ақаулар
Бақыланбайтын қайта жүктеу мен бағдарламалық қамтамасыз етуді пайдалану	Зиян келтіргіш бағдарламалық қамтамасыз ету
Парольдердің қорғалмаған кестесі	Пайдаланушының сәйкестендірілген ақпараттарды ауыстырып қоюы
Бағдарламалық қамтамасыз етудегі белгілі олқылықтар	Бағдарламалық қамтамасыз етуді авторизацияланбаған пайдаланушылардың пайдалануы
Қол жетімділік құқығын қате бөлу	Бағдарламалық қамтамасыз етуді заңсыз түрде пайдалану

Б-қосымшасы
(анықтамалық)
Аспаптық құралдар мен әдістер

Б.1. Аспаптық құралдар

Тәуекелдерді бағалау жүргізу және тәуекелдерді басқару үшін сұрау және жауаптармен сауалнамаларға негізделген қарапайым тәсілдерден бастап құрылымдық талдауды пайдаланатын әдістермен аяқтап түрлі әдістер әзірленді. Сатуда бағалау процесіне көмектесуге арналған түрлі аспаптық құралдар бар. Оларға автоматтандырылған (компьтерлік) және автоматтандырылмаған өнімдер де жатады.

Б.1.1 Тәуекелдерді бағалау құралдарын таңдауға арналған өлшемдер

Ұйым қандай әдісті және өнімді пайдаланбаса да олар кем дегенде құрамбірліктерді, құрамбірліктер арасындағы байланыс пен осы стандарттың 5 және 6-бөлімдерінде сипатталған процестерді ескерулері керек.

Бірінші рет тәуекелдерді бағалау процесін аяқтап осы процесс нәтижелерін (ресурстар мен олардың елеулігін бағалау, қауіпсіздік талаптары мен тәуекелдер деңгейлері, сондай-ақ сәйкестендірілген басқару құралдары) мысалы дерекқорда сақтап, құжаттау керек. Бағдарламалық қолдау құралдары осы жұмысты елеулі түрде жеңілдетуі, сондай-ақ барлық қайта бағалау бойынша барлық келешек әрекеттерді жеңілдетуі мүмкін.

Тәуекелдерді бағалау үшін құрал нені қамтамасыз етуі керек? Төменде берілген тізім тәуекелдерді бағалау үшін құралдарды таңдау кезінде ескеру керек критерийлер туралы кейбір болжам алуға мүмкіндік береді;

– Бұл құрал кемінде мынадай модульдер болуы мүмкін:

– деректерді жинау;

– талдау;

– қорытындылар шығару

Оның негізінде таңдалған құрал жұмыс істеп қызмет ететін әдіс ұйымның саясатын және тәуекелдерді бағалауға жалпы тәсілді көрсетуі керек.

Егер басқару барысында балама нұсқаларды салыстыруды орындау және басқарудың балама, сенімді және экономикалық тиімді құралдарды таңдау талап етілетін болса, онда осы процестің маңызды бөлігі нәтижелерді тиімді ұсыну болып табылады, сондықтан бұл құрал нәтижелерді түсінікті және нақты түрде берілуін қамтамасыз етуі керек.

– Деректерді жинау кезеңінде алынған ақпарат мұрағатын және аналитикалық деректер мұрағатын жүргізу мүмкіндігі тәуекелдерді немесе сұрауларды кейінгі бағалау жүргізу кезінде жарап қалуы мүмкін.

– Оны тиімді пайдалануда маңызды роль атқаратындықтан осы құралды сипаттайтын құжаттама қол жеткізімді болуы керек.

– Таңдалған құрал ұйымда пайдаланылатын бағдарламалық және аппараттық қамтамасыз етумен сыйысымды болуы керек.

– Автоматтандырылған құралдар, әдетте тиімді және қателіктерден бос болады, алайда олардың кейбіреулері орнату немесе пайдаланудың күрделі процестеріне ие болуы мүмкін, сондықтан оқыту мен қолдау бағдарламаларының қол жеткізімділігін қарастыру қажеттігі туындауы мүмкін.

– Осы құралды қолдану тиімділігі кейде пайдаланушы осы өнімді қаншалықты жақсы түсінгендігінен, сондай-ақ тиімді орнатудан және пайдаланылатын құрал пішініне тәуелді болады, сондықтан орнату мен пайдалану бойынша нұсқаулықтың болуы үлкен мәнге ие болады.

Б.2 Тәуекелдерді бағалау әдістерінің типтері мен мысалдары

Б.2.1 **Қатерлерді бағалау процесін шолу**

– Тәуекелдерді бағалау процестері 3-бөлімде сипатталған бірнеше кезеңдерден тұрады:

– ресурстарды сәйкестендіру және бағалау (5.1 және 5.2 қара);

– қауіпсіздік талаптарын сәйкестендіру және бағалау (яғни қауіптер мен осалдықтар, құқықтық талаптар мен бизнес талаптар, сондай-ақ 5.3 және 5.4 қара);

– тәуекелдерді есептеу (5.5 қара);

– тәуекелдерді өңдеудің тиісті нұсқасын сәйкестендіру (5.6-қара);

– тәуекелдерді қолайлы деңгейге дейін азайту үшін басқару құралдарын таңдау (5.7-қара).

Тәуекелдерді бағалау мақсаты қауіпсіздікті басқарудың тиісті және негізделген құралдарын кейіннен сәйкестендіру және таңдау үшін ақпараттық жүйе мен оның ресурстары түсетін тәуекелдерді сәйкестендіру мен бағалаудан тұрады. Бұл бағалау осы үлгімен ресурстар құнына және қауіпсіздік талаптарының деңгейлеріне негізделеді және басқарудың бар/жоспарланған құралдарын ескереді. Осы Қосымшада ол кезінде тәуекелдерді сәйкестендіру мен есептеу жүргізілетін тәуекелдерді бағалау процесінің бірінші бөлігі қарастырылады (5-бөлімде 5.1-5.5 кезеңдер).

Оқыс оқиға туындаған жағдайда ресурстар құнының мәндері немесе бизнеске әлеуетті әсер етулерді сандық (мысалы қаражаттық) және сапалы («орташа» немесе «жоғары» сияқты сипаттамаларға негізделе алатын) көрсеткіштерді, немесе олардың жиынтығын пайдалануды қоса бірнеше тәсілдермен бағалауға болады. Тәуекелдерді бағалау процесінің қиын бөлігі

қауіптер мен осалдықтарды бағалау болуы мүмкін. Қатердің жүзеге асырылу ықтималдығы мына факторларға тәуелді болады:

– ресурс тартымдылығы – егер адам тарапынан қасақана қатер қарастырылатын болса қолданылады;

– ресурс үшін сыйақы алу жеңілдігі – егер адам тарапынан қасақана қатер қарастырылатын болса, қолданылады;

– қатерді іске асыру үшін қажетті техникалық мүмкіндіктер - егер адам тарапынан қасақана қатер қарастырылатын болса, қолданылады;

– қатер ықтималдығы;

– пайдалануға осалдықты қабылдаушылық техникалық және сондай-ақ техникалық емес осалдықтарға да қолданылады.

Тәуекелдерді бағалаудың көптеген әдістерінде кестелер қолданылады және бірлесіп сапалық және сандық көрсеткіштер пайдаланылады. Бұрын айтылып кеткендей тәуекелдерді бағалаудың дұрыс және бұрыс әдістері болмайды. Бұдан басқа әдіс ҚР СТ ИСО/МЭК 27001 стандартында берілген талаптардың сақталуын қамтамасыз етуі керек, сондай-ақ ұйымның өзі үшін қолайлы, ұйым сенім артатын және қайталанатын нәтижелер алуға мүмкіндік беретін әдісті пайдаланғаны маңызды. Төменде кестелерге негізделген әдістердің бірнеше мысалдары берілген.

Б.2.2 Қатерлер/осалдықтарды жеке бағалауға арналған кестелер

Осы мысалда қатерлер мен осалдықтар оқыс оқиғалар себептері ретінде бірлесіп қарастырылмайды (5.3-те сияқты), ал жеке ескеріледі. Бұл мысалы [3] егжей-тегжей сипатталатын қатерлерді бағалаудың мүмкін тәсілінің бірі, сондай-ақ бірнеше аспаптық құралдармен қолданады. Егер бұл әдіс таңдалатын болса, құқықтық және бизнес талаптарды әбден қарастыру керек.

Ресурстарды бағалаулар ресурс құны мен маңыздылығын анықтауға мүмкіндік беретін ақпаратты нақты бере алатын бизнес –қызметкерлерден таңдалған қызметкерлерге («ресурс иелеріне») сауал қою нәтижелері бойынша алынады. Бұл сауалнама рұқсат етілмеген ашу, рұқсат етілмеген түрлендіру, өз іс-әрекетінен бас тарту, уақыттың түрлі кезеңдерінде қол жетпеушілік және жою сияқты оқыс оқиғалар нәтижесінде қалыпты болжалдар жағдайында іске асырылатын барынша қолайсыз нұсқалардан шығып ресурстар құны мен маңыздылығын бағалауды орындауға мүмкіндік береді.

Осы әдісте құқықтық және бизнес талаптарды ескеру үшін ресурстарды бағалау мынадай проблемаларды қамтуы керек:

– жеке қауіпсіздік;

– жеке ақпарат;

– құқықтық және нормативтік міндеттемелер;

– құқық қолдану;

– Коммерциялық және экономикалық мүдделер;
– Қаржылық шығындар/ жұмыс тоқтауы;
– Қоғамдық тәртіп;
– Бизнес-саясат және бизнес-операциялар;
– Материалдық емес шығындар.

Осы бағалау негізінде әр мүмкін зиян үшін және әр жеке ресурс үшін бағалаулар шкаласында сәйкес деңгейді анықтау керек, бұл мысалда 1-ден 4-ке дейінгі шкала қолданылады.

Келесі маңызды кезең әр ресурс үшін және осы ресурспен байланысты барлық қатерлер мен осалдықтар үшін қатерлер деңгейін (жүзеге асыру ықтималдығы) және осалдықтар деңгейлері (нәтижесінде оқыс оқиға болатын қатерлерді пайдалану жеңілдігі) үшін бағалаудың орындалуын қамтамасыз ету мақсатында сұрау парақтарын толтыру болып табылады. Әр сұраққа жауап бірнеше балл қосады. Бұл қатерлер деңгейлері мен осалдықтарды алдын ала берілген шкала бойынша сәйкестендіруге мүмкіндік береді (төменде берілген мысалда «Төмен – Орташа – Жоғары» шкала төменде кестеде көрсетілгендей пайдаланылады). Сұрау парақтарын толтыру кезінде пайдаланылатын ақпаратты лау үшін техникалық бөлім, кадрлар бөлімі және шаруашылық бөлімінің қызметкерлеріне сауалнама алу жүргізу, мүмкін физикалық орналасқан орынға инспекция жүргізу және бар құжаттаманы талдау жүргізу керек.

Ресурстар құнын бағалау төменде берілген кестеге ұқсас кесте көмегімен қатерлер мен осалдықтар деңгейлерімен салыстырылады. Әр жиынтық үшін 1-8 дейінгі шкала бойынша тиісті деңгей сәйкестендіріледі.

	Қатер деңгейі	Төмен			Орташа			Жоғары		
	Әлсіздік деңгейі	Н	С	В	Н	С	В	Н	С	В
Ресурстарды бағалау	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Әр ресурс үшін осы ресурсқа қатысты осалдықтар және оларға сәйкес қатерлер қарастырылады. Егер сәйкес қатерсіз осалдық болатын болса, немесе сәйкес осалдықсыз қатер болатын болса, онда тәуекел болмайды (бірақ егер жағдай өзгерсе сақ болған жөн). Кестеде сәйкес жол ресурсты бағалаумен сәйкестендіріледі, ал сәйкес бағана - қатер мен осалдық маңыздылығын көрсетеді. Мысалы егер ресурс 3 бағасына ие болса, қатер

деңгейі – «жоғары», ал осалдық деңгейі – «төмен» болса, онда тәуекел деңгейі 5 мәніне ие болады.

Кестеде қатерлер деңгейлері, осалдықтар деңгейлері мен ресурстарды бағалау санаттарының саны өзгеруі мүмкін және бұдан бұл кестені ұйым қажеттіктеріне сәйкес түзетуге болады. Қосымша бағаналар мен жолдарды пайдалану қатердің қосымша деңгейлерін тудырады. Бірінші ретте тәуекелдерді бағалау процесін аяқтап осы процесс нәтижелерін, мысалы дерекқорда сақтап құжаттау керек (ресурстар мен олардың маңыздылығының бағасы, қауіпсіздік деңгейлері мен қатерлер деңгейлері, сондай-ақ басқарудың сәйкестендірілген құралдары). Бағдарламалық қолдау құралдары осы жұмысты елеулі түрде жеңілдетуі, сондай-ақ барлық қайта бағалау бойынша барлық келешек әрекеттерді жеңілдетуі мүмкін.

Б.2.3 Қатер деңгейі бойынша оқиғаларды ұқсастыру

Әсер ету факторларын (ресурсты бағалау) және оқыс оқиға ықтималдығын (нақты оқыс оқиғаны тудыруы мүмкін қатерлер мен осалдықтарды немесе кез келген өзге қауіпсіздік талаптарын есепке алып) салыстыру үшін кестені пайдалануға болады. Бірінші адым 1-ден 5-ке дейінгі (төменде берілген кестенің «б» бағанасы) алдын ала белгіленген шкала бойынша әр ресурс үшін әсер етуді бағалаудан (ресурсты бағалаудан) тұрады. Екінші адымда әр оқыс оқиға үшін 1-ден 5-ке дейінгі (төменде берілген кестенің «в» бағанасы) алдын ала белгіленген шкала бойынша оқыс оқиға ықтималдығын бағалау керек. Үшінші адым (б х в) көбейту көмегімен қатер деңгейін есептеуден тұрады. Сонымен оқыс оқиғаларға олардың «әсер ету» коэффициентіне сәйкесетін санат беріле алады. Осы мысалда 1 ең кіші әсер ету мен ең кіші оқыс оқиға ықтималдығын білдіретіндігін атап кету керек.

Оқиғаны сәйкестендіруші (а)	Ықпал етуді бағалау (ресурсты) (б)	Оқиғаның пайда болу ықпалдылығына (в)	Қатер деңгейі (г)	Оқиға дәрежесі (д)
Оқиға А	5	2	10	2
Оқиға Б	2	4	8	3
Оқиға В	3	5	15	1
Оқиға Г	1	3	3	5
Оқиға Д	4	1	4	4
Оқиға Е	2	4	8	3

Жоғарыда көрсетілгендей бұндай процедура түрлі әсер ету мен түрлі ықтималдыққа ие түрлі оқыс оқиғаларды салыстыруға мүмкіндік береді және бұл мына жерде көрсетілген және олардың басымдылығына орай оларды ажыратуға мүмкіндік береді. Кейбір жағдайларда осы жерде

пайдаланылатын эмпирикалық шкалалармен ақша мәндерін байланыстыру керек.

Б.2.4 Жүйелер үшін қатерлерді бағалау

Осы мысалда оқыс оқиғалар мен олардың әсер етулерін есепке алып артықшылық берілуі керек жүйелерді анықтауға көңіл бөлінеді. Ол үшін ресурс пен әр қатер үшін екі баға анықталады, олар бірге әр ресурс үшін балл анықтауға мүмкіндік береді. Ақпараттық жүйе үшін қатер деңгейі барлық ресурстар бойынша баллдар жиынтығы ретінде есептеледі.

Бірінші әр ресурсқа кейбір бағалау беріледі. Бұл баға егер осы ресурс үшін қатерлерді іске асырған жағдайда туындауы мүмкін әлеуетті зиянды білдіреді. Бұл ресурсты бағалау ресурс түсірілетін әр қатер үшін ресурсқа беріледі.

Осыдан кейін ір оқыс оқиға үшін Б.2.3 сипатталғандай оқыс оқиға ықтималдығы бағаланады. Содан кейін ресурсты бағалау мен төменде берілген оқыс оқиға ықтималдығы мәнінің қиылысуын іздестіру көмегімен әр ресурс/оқыс оқиға үшін балл анықталады.

Ресурстарды бағалау	0	1	2	3	4
Оқиға ықтималдығы					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Қорытынды адымда осы жүйенің барлық ресурстары үшін қорытынды баллдар жинақталады, нәтижесінде жүйені бағалау алынады. Бұндай процедураны жүйені дифференциалдауды жүргізу және қорғанысы басым мәнге ие болуы керек жүйені анықтау үшін пайдалануға болады. Төменде мысал келтірілген.

Мысалы S жүйесі Al, А2 және А3 үш ресурстен тұрады. Бұдан басқа S жүйесінде туындауы мүмкін I1 және I2 екі оқыс оқиға бар. Al үшін баға 3-ке, А2 үшін – 2, А3 үшін – 4 тең болсын.

Егер А1 ресурсы үшін I1 оқыс оқиға ықтималдығы 1-ге тең болса, онда ресурс/оқыс оқиға А1/I1 баллы жоғарыда берілген кестеден 3-ке тең ресурсты бағалау мен 1-ге тең оқыс оқиға ықтималдығы ретінде алынуы мүмкін, яғни бұл балл 4-ке тең болады. Осы үлгімен егер А1 ресурсы үшін I2 оқыс оқиға ықтималдығы 3-ке тең болса, онда А1/I2 үшін балл 6-ға тең болады.

Осыдан кейін барлық оқыс оқиғалар бойынша А1 (Al_total) ресурсы үшін қорытынды баллды есептеуге, содан кейін – барлық ресурстар үшін

ұқсас қорытынды балл мен оларға қатысты қатерлерді есептеуге болады. Жүйе үшін қорытынды балл A1_total + A2_total + A3_total қосу көмегімен есептеледі.

Осы үлгімен жүйелерді салыстыруды орындау және олардың басымдылықтарын анықтауға болады.

Б.2.5 Қолайлы және қолайсыз қатерлерді ажырату

Қатерлер деңгейін анықтаудың тағы бір тәсілі тек қолайлы және қолайсыз қатерлерді ажыратудан тұрады. Осы әдістің негізі қатер деңгейлері олар үшін шараларды шұғыл қабылдау талап етілетін қатерлерді анықтау үшін ғана пайдаланылады.

Бұндай тәсіл жағдайында пайдаланылатын тәсіл тек сандардан ғана тұрмай, тек қатер қолайлы немесе қолайсыз болып табылатындығын көрсететін тек П және Н мәндерінен ғана тұратын болады. Мысалы Б.2.4 кесте мына үлгімен өзгереді:

Залалды бағалау	0	1	2	3	4
Оқиғаның ықтималдығы					
0	П	П	П	П	Н
1	П	П	П	Н	Н
2	П	П	Н	Н	Н
3	П	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Және бұл жағдайда осы кесте тек мысал болып табылады және пайдаланушы қолайлы және қолайсыз қатерлер арасында ажырату сызығын жүргізе алады.

Қосымшасы
(анықтамалық)
Библиография

[1] BS ISO/IEC TR 13335-1:1996 Guidelines for the Management of IT Security (GMITS) Part 1: Concepts and Models for IT Security – [BS ISO/IEC TR 13335-1:1996 АТ-қауіпсіздігін басқару жөніндегі нұсқаулық (GMITS), 1-бөлім: АТ-қауіпсіздігіне арналған тұжырымдар мен модельдер]

[2] BS ISO/IEC TR 13335-2:1997 Guidelines for the Management of IT Security (GMITS) Part 2: Managing and Planning IT Security – [BS ISO/IEC TR 13335-2:1997 АТ-қауіпсіздігін басқару жөніндегі нұсқаулық (GMITS), 2-бөлік: АТ-қауіпсіздігін басқару және жоспарлау]

[3] BS ISO/IEC TR 13335-3:1998 Guidelines for the Management of IT Security (GMITS) Part 3: Techniques for the Management of IT Security – [BS ISO/IEC TR 13335-3:1998 АТ-қауіпсіздігін басқару жөніндегі нұсқаулық (GMITS), 3-бөлік: АТ-қауіпсізідгіне арналған әдістер]

[4] BS ISO/IEC TR 13335-4:2000 Guidelines for the Management of ГГ Security (GMITS) Part 4: Selection of Safeguards – [BS ISO/IEC TR 13335-4:2000 АТ-қауіпсіздігін басқару жөніндегі нұсқаулық (GMITS), 4-бөлік: Қауіпсіздік шараларын таңдау]

[5] BS ISO/IEC PDTR 13335-5:2001 Guidelines for the Management of IT Security (GMITS) Part 5: Safeguards for External Connections [BS ISO/IEC PDTR 13335-5:2000 АТ-қауіпсіздігін басқару жөніндегі нұсқаулық (GMITS), 5-бөлік: Сыртқы қосылыстарға арналған қауіпсіздік шаралары]

[6] БИС РД 3002:2002 «BS 7799 стандарты бойынша тәуекелдерді бағалау және басқару бойынша жетекшілік» («Guide to BS 7799 risk assessment»)

[7] Protecting Business Information "Understanding the risks", published by the DTI, URN 96/939, 1996

[8] Protecting Business Information "Keeping it Confidential", published by the DTI, URN 96/938, 1996

[9] Information Security Assurance Guidelines for the commercial sector, published by the DTI, URN 99/697, 1999

[10] ISO Guide 73:2002 Risk Management – Vocabulary – Guidelines for use in standards

[11] OECD Guide on security for information systems and networks, September 2002

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: сертификаттау, стандарт талаптары, ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ), тәуекелдерді бағалау, басқару құралдары.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ

СТ РК 34.029 - 2008

Издание официальное

Комитет по техническому регулированию и метрологии
Министерства индустрии и торговли Республики Казахстан
(Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

4 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Общие положения

Настоящий стандарт предназначен тем, кто участвует:

– в разработке и сопровождении Системы управления информационной безопасностью (СУИБ),

– в подготовке к сертификации СУИБ,

– в аудите СУИБ организации (аудиты первой стороны – такие, как внутренние аудиты, аудиты второй стороны, например, аудиты, выполняемые аудиторами заказчиков и аудиты третьей стороны, например, аудиты, выполняемые независимыми органами сертификации).

Важно, что результаты действий по оценке рисков используются организацией для объяснения и обоснования, в особенности в качестве важнейшей части процесса сертификации, почему были выбраны конкретные цели управления и средства управления из Приложения А, почему некоторые из них не были выбраны и (при необходимости) почему были выбраны средства управления в дополнение к тем, которые перечислены в стандарте *СТ РК ИСО/МЭК 27001*.

Понятие СУИБ

Система управления информационной безопасностью (СУИБ) представляет собой часть общей системы управления, основанную на оценке бизнес-рисков и предназначенную для разработки, реализации, эксплуатации, мониторинга, сопровождения и совершенствования информационной безопасности. Система управления включает в себя организационную структуру, политики, разработку планов, распределение ответственности, инструкции, процедуры, процессы и ресурсы. Область применения СУИБ может быть определена в терминах организации как целого или частей организации, охватывая важнейшие ресурсы, системы, приложения, сервисы, сети и технологии, используемые для обработки, хранения и передачи информации. При этом сама информация рассматривается в качестве ресурса. В настоящем стандарте подобная совокупность связанных с информацией элементов называется «информационной системой» или «информационными системами». В таком контексте СУИБ может охватывать:

– все информационные системы организации;

– некоторые информационные системы организации;

– отдельную информационную систему.

Область применения СУИБ, определяемая организацией, является предметом сертификации, как указано в таблице в конце данного раздела. Возможно, организации потребуется определить различные СУИБ для различных подразделений или аспектов своего бизнеса. Например, можно определить СУИБ для конкретных торговых отношений с другой компанией.

Еще одним примером может быть структуризация организацией своего бизнеса для обеспечения необходимой классификации деловых партнеров, что может быть осуществлено с помощью одной или нескольких различных СУИБ. Возможны различные сценарии, которые могут быть охвачены одной или несколькими СУИБ.

Модель ПРОК

Модель, известная как «Планирование – Реализация – Оценка – Корректировка (Plan-Do-Check-Act)» (Модель ПРОК (PDCA)), используется в стандарте *СТ РК ИСО/МЭК 27001*. Данная модель используется в качестве основы для разработки, реализации, мониторинга, анализа, сопровождения и совершенствования СУИБ. Более подробная информация о данной модели приводится в стандартах *СТ РК ИСО/МЭК 27001* и *СТ РК*.

Структура настоящего стандарта

Настоящий стандарт состоит из двух частей:

– В первой части содержатся общие сведения о том:

– что такое информационная безопасность,

– почему необходимо принимать меры защиты,

– как добиться необходимой защиты.

– Во второй части приводится:

– описание компонентов оценки рисков и связей между ними,

– подробное описание того, что включается в процессы оценки рисков,

– описание различных вариантов общего подхода, или стратегии, которые могут быть реализованы организацией для оценки рисков.

Кроме того, стандарт содержит несколько приложений, в которых приводятся более подробные примеры угроз и уязвимостей по отношению к целям и средствам управления, включенным в стандарты *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001*, а также информация о методах и инструментальных средствах, используемых для оценки рисков и обработки рисков.

Область применения и цели стандарта *СТ РК ИСО/МЭК 17799*

Стандарт *СТ РК ИСО/МЭК 17799* предоставляет руководство по практическому применению управления информационной безопасностью. Главные цели стандарта заключаются в том, чтобы обеспечить:

– общую основу для организаций, разрабатывающих, реализующих и оценивающих управление безопасностью на практике;

– конфиденциальность деловых отношений между организациями.

В стандарте *СТ РК ИСО/МЭК 17799* определяется совокупность целей управления, а также полный набор средств управления безопасностью, которые могут быть реализованы для поддержки целей управления.

Эти средства управления рекомендуются для практического обеспечения информационной безопасности, с учетом, конечно же,

ограничивающих факторов, таких как ограничения, связанные с окружающей средой или используемыми технологиями. Некоторые средства управления не могут быть применены в каждой бизнес-среде и их следует использовать избирательно, в зависимости от локальных условий.

Область применения и цели стандарта *СТ РК ИСО/МЭК 27001*

Стандарт *СТ РК ИСО/МЭК 27001* определяет требования к разработке, реализации, эксплуатации, контролю, анализу, сопровождению и усовершенствованию документированной СУИБ в контексте общих бизнес-рисков организации. В данном стандарте определяются требования к реализации средств управления безопасностью, настраиваемых под потребности отдельных организаций или их частей.

СУИБ разрабатывается для обеспечения адекватных и соразмерных средств управления безопасностью, которые защищают информационные ресурсы и обеспечивают конфиденциальность для заинтересованных сторон. Это, в свою очередь, позволяет поддерживать и повышать конкурентоспособность, поток денежных средств, рентабельность, соответствие правовым требованиям и коммерческую репутацию.

Оценка рисков и выбор средств управления в контексте стандарта *СТ РК ИСО/МЭК 27001*

Организации необходимо выполнить оценку рисков, связанных с нарушениями безопасности, с учетом коммерческой ценности информации и других ресурсов, подвергающихся риску, для информационных систем, которые включены в область применения разрабатываемой и сопровождаемой СУИБ. Цели управления и средства управления, выбранные организацией и документированные в СУИБ в соответствии с конкретной ситуацией и условиями бизнеса, должны быть определены в результате процесса идентификации и оценки рисков нарушения безопасности с помощью процесса оценки рисков.

На основании результатов оценки рисков можно выбрать необходимые средства управления из Приложения А стандарта *СТ РК ИСО/МЭК 27001*, которые позволят защитить ресурсы организации, охваченные СУИБ, от идентифицированных рисков. Для получения сертификации СУИБ организация должна быть способна продемонстрировать адекватность целей управления и средств управления, выбранных для обеспечения информационной безопасности, идентифицированным рискам.

Средства управления, не включенные в стандарт *СТ РК ИСО/МЭК 27001*

Процесс выбора целей управления и средств управления не исключает идентификации и реализации средств управления, не приведенных в Приложении А стандарта *СТ РК ИСО/МЭК 27001*. Возможна ситуация, когда для оцененных рисков потребуется применение иных средств управления, чем те, которые приводятся в стандарте. Эти средства

управления могут быть выбраны из других каталогов средств управления, библиотек, стандартов и прочих источников. Для получения сертификации обоснование применения средств управления, не включенных в стандарт, должно быть документировано таким же образом, что и для средств управления, выбранных из стандарта *СТ РК ИСО/МЭК 27001*

Подробное описание процесса Планирование – Реализация – Оценка – Корректировка (Plan – Do –Check – Act)

В стандарте *СТ РК ИСО/МЭК 27001* описывается разработка и управление документированной СУИБ. Организации, стремящиеся получить сертификацию или повторную сертификацию соответствия стандарту, должны применять модель Планирование – Реализация – Оценка – Корректировка к процессам СУИБ, как описано в следующей таблице (более подробная информация приводится в данном документе):

Тема/Задача	Задача организации
Разработка СУИБ	а) Определить область применения СУИБ; б) Определить политику СУИБ; в) Определить систематический подход к оценке рисков; г) Идентифицировать риски; д) Оценить риски; е) Идентифицировать и оценить варианты обработки рисков; ж) Выбрать цели управления и средства управления; з) Подготовить Положение о применимости; и) Получить утверждение у руководства.
Реализация и эксплуатация СУИБ	а) Сформулировать положения плана обработки рисков; б) Реализовать план обработки рисков; в) Реализовать все выбранные цели управления и средства управления; г) Реализовать программы обучения и оповещения; д) Управлять эксплуатацией СУИБ; е) Управлять ресурсами для СУИБ.
Мониторинг и анализ СУИБ	а) Выполнять процедуры мониторинга; б) Осуществлять регулярный анализ эффективности СУИБ; в) Анализировать уровень остаточных рисков и идентифицированные приемлемые уровни рисков; г) Проводить внутренние аудиты СУИБ; д) Регулярно проводить анализ СУИБ управленческим персоналом; е) Регистрировать все события, которые могут повлиять на эффективность СУИБ.

Сопровождение и совершенствование СУИБ	а) Реализовывать идентифицированные усовершенствования; б) Принимать надлежащие корректирующие и превентивные меры; в) Информировать о результатах все заинтересованные стороны; г) Удостоверяться, что усовершенствования достигают поставленных целей.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ

Дата введения 2008.07.01.

1 Область применения

В настоящем стандарте рассматривается вопрос оценки рисков в контексте стандартов *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001*.

Цель настоящего стандарта – дать общее представление об используемой терминологии и основных понятиях, лежащих в основе процесса оценки рисков и всей процедуры, выполняемой при оценке рисков.

Настоящий стандарт предназначен организациям, которые:

- нуждаются в понимании процесса оценки рисков в контексте стандартов *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001*;
- разрабатывают и сопровождают свою Систему управления информационной безопасностью;
- готовятся к сертификации или повторной сертификации своей Системы управления информационной безопасностью.

Он также предназначен для использования организациями, участвующими в проведении сертификации, которым необходимо понять процесс оценки рисков.

Использование Руководств по управлению ИТ-безопасностью (Guidelines for the Management of IT Security) (GMITS)

«Руководства по управлению информационной безопасностью» (GMITS) – это разработанные ИСО/МЭК и признанные в международном масштабе руководства по управлению ИТ-безопасностью, информация из которых используется в различных местах настоящего стандарта. В GMITS определяется совокупность инструкций и методов управления безопасностью, разработанных и согласованных многими ведущими международными компаниями и организациями.

GMITS образуют базис для множества понятий, концепций и методов для процесса оценки и обработки рисков, описанных в настоящем стандарте. Хотя в названии стандарта GMITS говорится об ИТ-безопасности, его область применения выходит за эти рамки, поэтому принципы, указанные в данных руководствах, могут применяться и к информационной безопасности.

Издание официальное

В разделах 5 и 6 настоящего стандарта объясняется, каким образом рекомендации или инструкции, приведенные в различных разделах GMITS, могут быть использованы для поддержки процессов оценки и обработки рисков в случае общего применения стандартов ИСО/МЭК 17799 и ИСО/МЭК 27001 в сочетании с процессом сертификации по стандарту ИСО/МЭК 27001.

Ниже дается краткий обзор пяти различных частей стандарта GMITS (см. [1] - [5]).

Примечание – Необходимо применять самые последние издания и действующие редакции документов, упоминаемых в настоящем стандарте.

GMITS. Часть 1. Концепции и модели для ИТ-безопасности

В Части 1 стандарта GMITS описываются основные принципы и модели, которые должны быть приняты во внимание в процессе оценки рисков. Обзор этих принципов приводится в разделе 5. Пользователям настоящего стандарта, не знакомым с этими принципами, следует обратиться к стандарту GMITS, Часть 1 за более подробной информацией.

GMITS. Часть 2. Управление и планирование ИТ-безопасности

В Части 2 стандарта GMITS описываются различные действия, связанные с управлением ИТ-безопасностью в организации. Эта часть может быть использована при выборе стратегий управления и назначении ответственных в процессе обеспечения ИТ-безопасности. Кроме того, в ней описываются различные этапы планирования, разработки политики безопасности, оценки рисков, реализации средств управления и сопровождения ИТ-безопасности с точки зрения руководства. Как и в случае Части 1 стандарта GMITS, пользователям настоящего стандарта следует обратиться за более подробной информацией к Части 2.

GMITS. Часть 3. Методы управления для ИТ-безопасности

В Части 3 стандарта GMITS обсуждаются и рекомендуются методы, используемые для успешного управления ИТ-безопасностью. К ним относятся различные варианты оценки рисков, описанные в разделе 6, и процесс оценки рисков, описанный в разделе 5, включая подробное описание различных возможностей оценки рисков в Приложении. Поэтому Часть 3 стандарта GMITS может использоваться для получения более подробной информации на указанные темы, особенно о том, как выполнять оценку рисков.

GMITS. Часть 4. Выбор мер обеспечения безопасности

В Части 4 стандарта GMITS приводится информация о выборе средств управления, в зависимости от различных методов оценки (как, например, описано в Разделе 4). Часть 4 может помочь при выборе средств управления из практических руководств, таких как *СТ РК ИСО/МЭК 17799*, а также при

выборе средств управления в соответствии с детальной оценкой рисков. Эту часть можно использовать при выборе средств управления, описанных в Разделе 5 настоящего стандарта.

GMITS. Часть 5. Меры обеспечения безопасности для внешних соединений

В Части 5 стандарта GMITS приводятся инструкции для организации, подключающей свои информационные системы к внешним сетям. В этой части описывается выбор и использование средств управления безопасностью, позволяющих обеспечить безопасность для внешних соединений и сервисов, поддерживаемых этими соединениями. Кроме того, в ней описываются дополнительные средства управления, необходимость которых обуславливается этими соединениями. Часть 5 может использоваться также и при выборе средств управления безопасностью из стандарта *СТ РК ИСО/МЭК 17799*, в случае если используются внешние соединения.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.

СТ РК ИСО/МЭК 27001-2008 Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования.

3 Термины и определения

В настоящем стандарте применяются термины по [1], [9], *СТ РК ИСО/МЭК 17799*, *СТ РК ИСО/МЭК 27001*, а также следующие термины с соответствующими определениями:

Информация (information): Смысловое значение, которое в данный момент присвоено данным через условные соглашения, применяемые к этим данным.

Политика информационной безопасности (information security policy): Правила, инструкции и практические нормы, определяющие, каким образом управляются, защищаются и распространяются ресурсы, включая критичную информацию.

Ресурс (asset): Все, что представляет ценность для организации, ее бизнес-операций и их непрерывности.

Средство управления безопасностью (security control): Практическая норма (practice), процедура или механизм, которые позволяют уменьшить риски безопасности.

Управление информационной безопасностью (information security management): Предоставление механизма, позволяющего реализовать информационную безопасность.

Примечание – Управление рисками обычно включает оценку рисков, обработку рисков, принятие рисков и передачу рисков.

4 Основные положения

4.1 Сущность информационной безопасности

Цель информационной безопасности состоит в обеспечении непрерывности бизнеса и в минимизации ущерба бизнесу с помощью предотвращения и минимизации воздействия инцидентов информационной безопасности.

Управление информационной безопасностью позволяет коллективно использовать информацию, обеспечивая при этом защиту информации и всех прочих ресурсов в пределах области применения СУИБ (см. 5.1). Информационная безопасность должна обеспечить три основных компонента:

- Конфиденциальность: защита важной информации от неавторизованного раскрытия и перехвата информации в читаемом виде;
- Целостность: защита точности и полноты информации и программного обеспечения;
- Доступность: обеспечение доступности информации и важнейших сервисов для пользователей.

Информация имеет множество форм. Она может храниться на компьютерах, передаваться по сетям, распечатываться или записываться на бумаге или произноситься в речевом общении. С точки зрения обеспечения безопасности необходимая защита должна применяться ко всем формам информации, включая печатные документы, базы данных, пленки, презентации, магнитные ленты, дискеты, компакт-диски, разговоры (например, разговоры с использованием таких технологий, как стационарные и мобильные телефоны) и все другие методы и носители информации, используемые для передачи знаний и идей.

4.2 Необходимость принятия мер

Информация, принадлежащая организации, а также системы, приложения и сети, поддерживающие эту информацию, являются важными бизнес-ресурсами. Конфиденциальность, целостность и доступность ресурсов могут иметь большое значение для поддержания конкурентоспособности, потока денежных средств, рентабельности, соответствия правовым требованиям и коммерческой репутации. Организация может столкнуться с увеличением числа угроз безопасности из различных

источников. Системы, приложения и сети, принадлежащие организации, могут оказаться целью ряда серьезных угроз (см. 5.3), включая мошенничество с применением компьютеров, шпионаж, саботаж, вандализм и другие источники отказов в работе или аварий. Продолжают появляться новые источники возможного ущерба, такие как широко обсуждаемые угрозы от компьютерных вирусов и компьютерных хакеров. Ожидается, что подобные угрозы, которым подвергается информационная безопасность, станут еще более распространенными, более претенциозными и более изощренными. В то же самое время, в результате возросшей зависимости от технологий, основанных на информационных системах и сервисах, организация может стать более уязвимой к угрозам безопасности.

Более широкое использование сетевых технологий предоставляет новые возможности для неавторизованного доступа к компьютерным системам, а тенденция к распространению вычислительной техники сокращает область действия осуществляемого специалистами централизованного контроля СУИБ организации.

Для отражения подобных угроз необходимо идентифицировать и реализовать соответствующие цели управления и средства управления, позволяющие обеспечить защиту принадлежащей организации информации. В этом отношении стандарты *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001* предоставляют хороший источник средств управления для выполнения данного требования и для разработки систем управления информационной безопасностью. Чтобы идентифицировать и выбрать необходимые средства управления, организация должна идентифицировать свои требования безопасности (см. 5.3 и 5.4) к информационным системам, включенным в СУИБ, в контексте своих бизнес-процессов и приложений.

Уязвимы к угрозам безопасности организации всех видов деятельности и всех размеров, от многонациональных корпораций до предприятий среднего и малого бизнеса. Чем скорее будут приняты меры по защите принадлежащей организации информации, тем более дешевой и более эффективной окажется безопасность организации со временем.

4.3 Общее представление о процессе оценки рисков

Как правило, средства и методы оценки рисков применяются ко всей СУИБ или к конкретным информационным системам и техническим средствам, но также, если это является практичным, реалистичным и полезным, они могут быть направлены на отдельные системные компоненты или сервисы. Оценка рисков включает в себя систематический анализ следующих аспектов:

Последствия – ущерб для бизнеса, который может возникнуть в результате значительного нарушения информационной безопасности, с

учетом возможных последствий потери или недостаточного обеспечения конфиденциальности, целостности и доступности информации;

Вероятность – реальная вероятность того, что подобное нарушение произойдет в свете превалирующих угроз, уязвимостей и средств управления.

Этот процесс включает в себя:

Выбор метода оценки рисков (см. раздел 6), подходящего для данной СУИБ, идентификацию требований к безопасности бизнес-информации, правовых и нормативных требований, а также определение критериев для принятия рисков и идентификация приемлемых уровней рисков.

Идентификацию и оценку рисков (см. раздел 5) для системы (систем) управления информационной безопасностью и информационных систем, входящих в СУИБ; идентификацию и оценку вариантов обработки рисков, выбор целей управления и средств управления для уменьшения рисков до приемлемых уровней, а также – для сертификации - подготовка Положения о применимости.

Каждая организация, которая хочет реализовать адекватные средства управления безопасностью, должна использовать результаты оценки рисков для определения необходимых действий по обработке действий и определения приоритетов для управления рисками информационной безопасности. Этот процесс позволяет организации идентифицировать подлежащие реализации и применению необходимые средства управления из стандартов *СТ РК ИСО/МЭК 17799* или *СТ РК ИСО/МЭК 27001*, Приложение А, соответственно. Оценка рисков зависит от следующих факторов:

- типа бизнес-информации и систем;
- цели деятельности, с которой используется данная информация;
- среды окружения, в которой используется и функционирует система;
- защиты, обеспечиваемой уже реализованными средствами управления.

В процессе оценки рисков могут быть идентифицированы исключительные риски безопасности, требующие реализации более мощных средств управления в дополнение к рекомендациям, приведенным в стандарте *СТ РК ИСО/МЭК 27001*. Выбор этих средств управления должен быть обоснован на основе результатов оценки рисков. Расходы на средства управления информационной безопасностью должны соответствовать коммерческой ценности информации и других подвергающихся рискам бизнес-ресурсов. Кроме того, эти расходы должны быть сбалансированы по отношению к воздействиям на бизнес, которые могут оказать нарушения безопасности. По этой причине периодический анализ бизнес-рисков и средств управления безопасностью, позволяющий учесть изменение бизнес-требований и приоритетов, является регулярно используемой функцией управления информационной безопасностью.

Ресурсы, необходимые для процесса оценки рисков и управления рисками, могут различаться в зависимости от глубины проводимого анализа, от требований безопасности и от сложности бизнеса организации.

Как показывает опыт, следующие факторы часто являются критичными для успешной реализации информационной безопасности в организации:

цели безопасности и действия, основывающиеся на целях и требованиях бизнеса и выполняемые руководством организации;

очевидная поддержка и приверженность (заинтересованность) со стороны высшего руководства;

хорошее понимание рисков безопасности;

эффективное продвижение безопасности до уровня менеджера и сотрудника;

распространение всеобъемлющих руководств по политике и стандартам информационной безопасности до всех сотрудников и подрядчиков.

4.4 Оценка рисков и обработка рисков в модели ПРОК (PDCA)

При взгляде на модель ПРОК и действия, которые должны быть выполнены в процессе СУИБ, становится очевидно, что оценка рисков является главной частью этапа «Планирование» в рамках модели ПРОК. Обработка рисков составляет важную часть этапа «Реализация» модели ПРОК. Если организация принимает решение подать заявку на сертификацию, то это следует делать только после выполнения всех действий этапа «Реализация».

Хотя это, возможно, и не так очевидно, но очень важно отметить, что в этап «Оценка» входят действия по повторной оценке всех рисков с целью проверить, что все реализованные средства управления эффективно уменьшают риски. Часть действий на этапе «Корректировка» представляет собой не что иное, как обработку повторно оцененных рисков, что делает этот этап похожим на этап «Реализация». Это означает, что оценка рисков и обработка рисков, описываемые далее в настоящем стандарте, помогают поддерживать все этапы модели ПРОК.

5 Процесс оценки рисков

Оценка рисков состоит из следующих этапов:

идентификация и определение ценности ресурсов (см. 5.1 и 5.2);

идентификация всех требований безопасности, т.е. угроз и уязвимостей, правовых и бизнес-требований (см. 5.3);

оценка вероятности появления угроз и уязвимости, а также оценка важности правовых и бизнес-требований (см. 5.4);

расчет риска, возникающего в результате указанных факторов (см. 5.5);

выбор необходимого варианта обработки риска (см. 5.6);

выбор средств управления для уменьшения рисков до приемлемого уровня (см. 5.7).

5.1 Идентификация ресурсов

Ресурсом является нечто, что обладает ценностью или полезностью для организации, ее бизнес-операций и их непрерывности. Поэтому, ресурсам требуется защита, которая позволит обеспечить корректное выполнение бизнес-операций и непрерывность бизнеса. Надлежащее управление ресурсами и их учет[1] имеют важнейшее значение для поддержания безопасности ресурсов организации. Эти два аспекта должны быть главной обязанностью на всех уровнях управления[2]. Важно, чтобы при инвентаризации учитывались основные ресурсы. Для уверенности в том, что нет пропущенных или забытых ресурсов, следует определить область применения рассматриваемой СУИБ в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий.

Каждый ресурс в границах данной области применения должен быть явным образом идентифицирован и соответствующим образом оценен (см. 5.2), а его владелец и категория безопасности должны быть согласованы и документированы (см. [6],[7], *СТ РК ИСО/МЭК 17799*). К ресурсам относится, например, следующее:

Информационные ресурсы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, процедуры эксплуатации и поддержки, планы обеспечения бесперебойной деятельности, средства аварийного восстановления;

Печатные документы: контракты, руководства, документация компании, документы с важными бизнес-результатами;

Программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, средства разработки и утилиты;

Физические ресурсы: вычислительное оборудование и аппаратура связи, магнитные носители информации (ленты и диски), другое техническое оборудование (источники питания, кондиционеры), мебель, помещения;

Люди: персонал, заказчики, абоненты;

Имидж и репутация компании;

---

[1] *В стандарте СТ РК ИСО/МЭК 17799 определяются две конкретные цели в отношении ресурсов: (i) 5.1 Учет ресурсов, и (ii) 5.2 Классификация информации.*

[2] У*чет ресурсов помогает обеспечить надлежащее поддержание информационной безопасности. Для основных ресурсов должны быть идентифицированы владельцы, на которых должна быть возложена ответственность за поддержание необходимых средств управления безопасностью. Ответственность за реализацию средств управления безопасностью может быть делегирована, в то время как учет должен оставаться обязанностью назначенного владельца ресурса.*

Сервисы и службы: вычислительные и коммуникационные сервисы, другие технические службы (отопление, освещение, электропитание, кондиционирование).

Результат этапа 5.1:

Результатом данного этапа должен быть реестр, в котором должны быть указаны все основные ресурсы, относящиеся к рассматриваемой СУИБ, их местонахождение и их владелец.

5.2 Оценка ресурсов

Идентификация и оценка ресурсов, основанная на бизнес-потребностях организации, является главной составляющей оценки рисков. Чтобы идентифицировать необходимую защиту для ресурсов, необходимо определить их ценность на основе их важности для бизнеса и их потенциальной значимости в определенных обстоятельствах. Эта значимость обычно определятся в терминах потенциальных воздействий на бизнес, которые могут оказать в результате нежелательные инциденты, такие как раскрытие, модификация, недоступность и/или уничтожение информации и других ресурсов. Эти инциденты могут, в свою очередь привести к финансовым потерям, к уменьшению прибыли, доли на рынке или к ущербу репутации компании.

Входные данные для оценки ресурсов должны быть предоставлены владельцами и пользователями ресурсов, которые способны авторитетно сообщить о важности ресурсов, особенно информации, для организации и ее бизнеса.

Полученные оценки должны соотноситься со стоимостью приобретения и поддержания ресурса, а также с воздействиями, которые может оказать потеря конфиденциальности, целостности и доступности на бизнес организации. Чтобы единообразно определить ценность ресурсов и надлежащим образом связать эти оценки, необходимо применять шкалу оценок ресурсов.

Для каждого ресурса должна быть идентифицирована ценность, которая показывает воздействие на бизнес в случае нарушения конфиденциальности, целостности или доступности, или любого другого важного свойства[3] ресурса. В качестве подобной шкалы оценивания можно, например, использовать:

Различие между низким, средним и высоким уровнем;

---

[3] *Иногда одних только критериев «конфиденциальности», «целостности» и «доступности» недостаточно для определения важности ресурса (например, при рассмотрении информации, для которой требуется защита права на интеллектуальную собственность). В таких случаях следует вводить дополнительные критерии, которые будут удовлетворять этим требованиям.*

Более подробную шкалу: пренебрежимый – низкий – средний – высокий – очень высокий;

Организация должна определить свои собственные границы для шкалы оценок ресурсов. Решение, что следует считать ущербом «низкого» или «высокого» уровня, является делом только самой организации – ущерб, который может быть катастрофическим для небольшой организации, может быть низким или даже пренебрежимым для очень крупной организации.

Правильное и понятное объяснение этих оценок в терминах бизнеса организации очень важно при разговоре с владельцами и пользователями, который должен состояться с целью получения входных данных для оценки ресурсов.

Результат этапа 5.2:

В результате данного этапа в реестр ресурсов должна быть добавлена оценка для каждого идентифицированного ресурса по каждому критерию, например, по конфиденциальности, целостности и доступности, а также по любым другими критериям, если они используются.

5.3 Идентификация требований безопасности

5.3.1 Источники требований

Требования безопасности в любой организации, независимо от размера, в действительности, выводятся из трех основных источников, которые должны быть документированы в СУИБ:

Уникальная совокупность угроз и уязвимостей, возникновение которых может привести к значительным потерям в бизнесе;

Правовые требования и договорные обязательства, которые должны выполняться организацией, ее торговыми партнерами, подрядчиками и поставщиками услуг;

Уникальный набор принципов, целей и требований по обработке информации, разработанный организацией для поддержки бизнес-операций и бизнес-процессов и применения к информационным системам организации.

После идентификации указанных требований безопасности, полезно сформулировать их в терминах требований к конфиденциальности, целостности и доступности.

В некоторый момент – либо до начала действий по оценке рисков, либо перед началом данного этапа – необходимо идентифицировать уже реализованные средства управления безопасностью. Это требуется для полной идентификации и реалистичной оценки угроз и уязвимостей, а также важно для выбора дополнительных средств управления (см. Этап 5.6), которые хорошо взаимодействуют с уже существующими. Настоящий стандарт предоставляет возможность проверки существующего состояния

безопасности относительно стандартов *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001*.

5.3.2 Идентификация угроз и уязвимостей

Ресурсы подвергаются угрозам различных типов. Угроза способна привести к нежелательному инциденту, который может стать причиной ущерба системе или организации и ее ресурсам. Этот ущерб может возникнуть в результате прямой или непрямой атаки на принадлежащую организации информацию, например, в результате неавторизованного уничтожения информации, ее раскрытия, модификации, повреждения, а также недоступности или потери. Угрозы могут возникать по причине случайных или преднамеренных источников или событий. Для нанесения ущерба ресурсам угрозе необходимо использовать какую-либо уязвимость систем, приложений или сервисов, используемых организацией. Примеры угроз приводятся в Приложениях А.1 и А.2 настоящего стандарта, а в [8] и [9] приводится дополнительная информация об угрозах.

Уязвимости представляют собой слабые места, связанные с ресурсами организации. Эти слабые места могут быть использованы угрозами, что может привести к потере, повреждению или причинению ущерба данным ресурсам. Сама по себе уязвимость не может причинить ущерб, это просто условие или ряд условий, которые могут позволить угрозе воздействовать на ресурс. При идентификации уязвимостей следует идентифицировать слабые места, которые могут быть использованы источником угрозы с целью нанесения ущерба ресурсам и поддерживаемому им бизнесу и которые связаны с ресурсами в:

- физической среде,
- процедурах и средствах управления, связанных с персоналом, управлением и администрированием,
- аппаратном и программном обеспечении, оборудовании и средствах связи.

Примеры уязвимостей приводятся в Приложении А.3 настоящего стандарта, а в [3]приводится дополнительная информация об уязвимостях.

Необходимо обратить внимание: В зависимости от используемого метода оценки рисков (см. раздел 6 и Приложение Б.2), угрозы и уязвимости оцениваются вместе или отдельно. Возможно использование обоих вариантов, и решение об их выборе следует принимать при выборе общего подхода к оценке рисков.

5.3.3 Правовые, нормативные требования и договорные обязательства

В СУИБ должны быть документированы требования безопасности, связанные с совокупностью правовых требований и договорных обязательств, которые должны выполняться организацией, ее торговыми

партнерами, подрядчиками и поставщиками услуг. Поддержка СУИБ этих требований имеет большое значение, например, для осуществления контроля копирования патентованного программного обеспечения, защиты документов организации или защиты данных. Очень важно, чтобы наличие или отсутствие средств управления безопасностью в каждой из информационных систем не нарушало ни одно из правовых или гражданских обязательств, а также ни один коммерческий договор. Поэтому необходимо идентифицировать правовые требования и договорные обязательства, связанные с каждым ресурсом.

5.3.4 Принципы, цели и бизнес-требования организации

Кроме того, в СУИБ должны быть документированы требования безопасности, связанные с принципами, целями и требованиями, применяемыми во всей организации для обработки информации с целью поддержки бизнес-операций организации. Поддержка СУИБ этих требований имеет большое значение, например, для повышения конкурентоспособности, денежных потоков и/или рентабельности. Очень важно, чтобы наличие или отсутствие средств управления безопасностью в каждой из информационных систем не препятствовало эффективному выполнению бизнес-операций. Поэтому для каждого ресурса необходимо идентифицировать связанные с ним бизнес-цели и бизнес-требования.

Результат этапа 5.3:

В результате этапа 5.3 для каждого ресурса, идентифицированного на этапе 5.1, должен быть составлен список идентифицированных угроз и уязвимостей, правовых требований/договорных обязательств и бизнес-требований.

5.4 Оценка требований безопасности

Как и при оценке ресурсов, в случае оценки требований безопасности необходимо определить шкалу для этой оценки, которая соответствовала бы используемому методу оценки рисков (см. раздел 6). В большинстве случаев, чтобы слишком не усложнять данный процесс, достаточно использовать простую трехуровневую шкалу, например:

низкий уровень
средний уровень
высокий уровень.

5.4.1 Оценка угроз и уязвимостей

После идентификации угроз и уязвимостей необходимо оценить вероятность реализации некоторой комбинации угроз и уязвимостей.

Необходимо обратить внимание: В зависимости от того, как оцениваются угрозы и уязвимости – вместе или отдельно, следует

использовать отдельную оценку угроз и уязвимостей или же совместную оценку.

При оценке вероятности угроз следует принять во внимание:

Для преднамеренных угроз: мотивацию, воспринимаемые и требуемые возможности, ресурсы, доступные потенциальным нарушителям, и понимание привлекательности ресурсов;

Для случайных (непреднамеренных) угроз: насколько часто они могут возникать, в соответствии с опытом, статистикой и т.д.; географические факторы, такие как близость к химическим и нефтеперерабатывающим заводам, нахождение в районах, где велика вероятность экстремальных погодных условий; и факторы, которые могут вызвать человеческие ошибки и нарушение работоспособности оборудования.

Полная вероятность появления инцидента зависит также от уязвимости ресурсов, т.е. от того, насколько легко их можно использовать. Следовательно, уязвимости должны быть оценены по некоторой шкале, например, следующей:

Высоковероятная или вероятная – данную уязвимость легко использовать, защита отсутствует или очень слаба;

Возможная – уязвимость может быть использована, но имеется защита;

Маловероятная или невозможная – данную уязвимость использовать трудно, имеется хорошая защита.

Информация, используемая для оценки угроз и уязвимостей, может быть получена от тех, кто имеет отношение к рассматриваемой СУИБ и соответствующим бизнес-процессам. Это могут быть, например, сотрудники отдела кадров, специалисты по планированию и ИТ-специалисты, а также те, кто отвечает в организации за безопасность. Кроме того, можно использовать списки угроз и уязвимостей (например, в Приложении А и в [3]), а также связи между угрозами и средствами управления из стандарта *СТ РК ИСО/МЭК 17799*, приведенные в Приложении А настоящего стандарта.

5.4.2 Оценка правовых требований и бизнес-требований

Таким же образом, как были оценены угрозы и уязвимости, теперь следует определить оценку для правовых требований и бизнес-требований (см. 5.3.3 и 5.3.4). Это необходимо для расчета рисков, связанных с этими требованиями безопасности.

Чтобы присвоить оценку какому-либо правовому или бизнес-требованию, необходимо определить:

насколько серьезным будет воздействие на бизнес в случае невыполнения данного правового требования/договорного обязательства или бизнес-требования;

какие последствия это может иметь для рассматриваемого ресурса и для всей СУИБ;

какова вероятность, что это произойдет.

Результаты анализа указанных факторов следует использовать для того, чтобы для каждого ресурса и каждого правового требования/договорного обязательства и каждого бизнес-требования определить соответствующую оценку на шкале оценок для требований безопасности.

Результат этапа 5.4:

В результате данного этапа всем идентифицированным требованиям безопасности должна быть присвоена некоторая оценка (см. также Этап 5.3 выше).

5.5 Расчет рисков безопасности

Цель оценки рисков заключается в идентификации и оценке рисков на основании результатов, полученных на этапах 5.1-5.4. Эти риски рассчитываются из комбинации оценок ресурсов и оцененных уровней соответствующих требований безопасности.

Существуют различные способы, позволяющие связать эти факторы; например, оценки, присвоенные активам, уязвимостям и угрозам, а также правовым и бизнес-требованиям, объединяются, в результате чего получаются значения степени риска. Несколько различных способов получения этих значений описываются в Приложении Б.2 «Типы и примеры методов оценки рисков». Эти методы основываются на понятиях, описанных в разделе 5.

Важно отметить, что не существует «правильных» или «неправильных» способов расчета рисков, при условии, что понятия, описанные в предыдущих разделах, объединяются некоторым осмысленным образом, и только сама организация может принять решение о том, какой метод оценки рисков подходит к ее бизнес-требованиям и требованиям безопасности.

Результат этапа 5.5:

В результате данного этапа для каждого ресурса, находящегося в области применения рассматриваемой СУИБ, должен быть составлен список измеренных рисков для каждого из воздействий, проявляющегося в форме раскрытия, модификации, недоступности и уничтожения.

5.6 Идентификация и оценивание вариантов обработки рисков

После того как риски идентифицированы и оценены, следующей задачей организации является идентификация и оценка самого подходящего действия для обработки этих рисков. Это решение должно приниматься на основе информации об охватываемых ресурсах, а также воздействий на бизнес. Еще одним важным фактором, лежащим в основе данного решения,

является приемлемый уровень риска, который был идентифицирован после выбора необходимого метода оценки рисков (см. раздел 6).

Для идентифицированных и оцененных рисков (в результате действий, описанных на этапах 5.1–5.5) существуют четыре возможных действия, которые может предпринять организация:

- применение надлежащих средств управления для уменьшения этих рисков (см. Раздел 5.7);
- сознательное и намеренное принятие рисков, при условии, что они явно удовлетворяют политикам организации и критериям принятия рисков (см. Раздел 6);
- предотвращение рисков (см. 5.6.1);
- передача ассоциированных бизнес-рисков другим сторонам (см. 5.6.2).

Перечисленные варианты должны быть оценены для каждого риска с целью определения наиболее подходящего варианта. Результаты этой деятельности следует документировать и впоследствии использовать при разработке плана обработки рисков.

5.6.1 Предотвращение рисков

К предотвращению рисков относятся все действия, в результате которых ресурсы исключаются из рискованных областей (например, физических областей или бизнес-процессов). Этого можно достичь, например, следующим образом:

невыполнение отдельных бизнес-операций (например, неиспользование средств электронной коммерции или неиспользование сети Интернет для конкретных бизнес-операций);

перемещение ресурсов из области, подвергающейся риску (например, запрет хранить важные файлы в сети Интранет организации или перемещение ресурсов из областей, в которых отсутствует надлежащая физическая защита);

решение не обрабатывать особо важную информацию, например, третьей стороной, если не может быть гарантировано должное обеспечение защиты.

При оценивании варианта предотвращения рисков, его необходимо сбалансировать с бизнес-потребностями и финансовыми затратами. Например, использование сети Интернет для электронной коммерции может быть обязательным вследствие потребностей бизнеса, несмотря на все проблемы, связанные с хакерами, а перемещение ресурсов в более безопасное место может быть недопустимо с точки зрения бизнес-процесса. В подобных ситуациях следует рассмотреть другие опции, т.е. передачу рисков и уменьшение рисков.

5.6.2 Передача рисков

Передача рисков может быть наилучшим вариантом в случае, если невозможно предотвратить риск и трудно, или слишком дорого, добиться уменьшения риска. Например, передача риска может быть осуществлена с помощью страхования на сумму, соизмеримую с оцененной стоимостью ресурсов и соответствующими рисками, а также с учетом важности ресурсов для бизнес-процессов организации.

Еще одна возможность состоит в использовании для работы с критически важными бизнес-ресурсами или процессами третьей стороны или аутсорсинговых партнеров, если они должным образом оснащены для выполнения подобной работы. В этом случае необходимо позаботиться, чтобы в соответствующие договора были включены все требования безопасности, цели управления и средства управления, которые гарантировали бы обеспечение необходимой безопасности. При этом нужно не забывать, что в большинстве случаев окончательная ответственность за безопасность передаваемых на аутсорсинг информации и средств обработки информации остается на первоначальной организации.

Еще одним примером передачи рисков может быть ситуация, когда ресурсы, которые подвергаются риску, выводятся за область применения данной СУИБ. В этом случае обеспечение защиты особо важной информации может оказаться более простым и дешевым, но необходимо позаботиться о том, чтобы все ресурсы, необходимые для бизнеса, были включены в данную СУИБ посредством интерфейсов и зависимостей.

Результат этапа 3.6:

В результате данного этапа должен быть идентифицирован и документирован наиболее подходящий вариант обработки рисков для всех рисков, которые были оценены с помощью процессов, описанных на этапах 5.1 - 5.5.

5.7 Выбор средств управления безопасностью

5.7.1 О выборе средств управления безопасностью

Чтобы уменьшить оцененные риски в пределах области применения рассматриваемой СУИБ, необходимо идентифицировать и выбрать необходимые и обоснованные средства управления безопасностью. Средства управления могут быть выбраны из стандартов *СТ РК ИСО/МЭК 17799* или *СТ РК ИСО/МЭК 27001*, Приложения А, а также из дополнительных источников. Целью выбора средств управления является уменьшение рисков до уровня, приемлемого для данной организации. Этот выбор должен основываться на результатах оценки рисков, например, уязвимости вместе с соответствующими угрозами показывают, где может потребоваться защита и в какой форме ее следует реализовать. Связь с оценкой рисков следует

документировать (особенно в целях сертификации), чтобы обосновать выбор (или противоположное решение) средств управления.

Уже реализованные средства управления должны быть подвергнуты переоценке на основе сравнений затрат, включая сопровождение, с намерением исключить или усовершенствовать их в случае недостаточной эффективности. Здесь следует отметить, что иногда исключение несоответствующего средства управления может быть более дорогостоящим, чем оставление его на месте с возможным добавлением другого средства управления. В случае если была выполнена предшествующая оценка рисков, то этот процесс должен включать результаты этапа «Оценка» в модели ПРОК.

При выборе средств управления для реализации следует рассмотреть множество факторов, в том числе:

- легкость использования средства управления,
- прозрачность для пользователя,
- помощь, предоставляемую пользователям для выполнения их функций,
- относительную мощность средств управления,
- типы выполняемых функций – предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг и оповещение.

Обычно средство управления выполняет сразу несколько перечисленных функций, и чем больше функций оно будет выполнять, тем лучше. Во время проверки общей безопасности, или совокупности подлежащих реализации средств управления, следует соблюдать баланс, если это вообще возможно, между указанными типами функций. Эта мера поможет реализовать более эффективное и рациональное обеспечение общей безопасности. Кроме того, при выборе средств управления всегда следует учитывать баланс между операционными (нетехническими) и техническими средствами управления, которые поддерживают и дополняют друг друга. К операционным средствам управления относятся те, которые обеспечивают физическую, кадровую и административную безопасность.

Кроме очень важного фактора уменьшения рисков (см. 5.7.2), при выборе средств управления следует также рассмотреть фактор стоимости. Будет неуместно рекомендовать средства управления, реализация и поддержание которых обойдется дороже, чем ранее согласованный бюджет, выделенный на обеспечение безопасности, поэтому необходимо попробовать найти более дешевые альтернативные варианты. Однако следует проявлять большую осторожность, если подобный бюджет приводит к уменьшению количества или качества средств управления, выбранных для реализации, поскольку это может привести к нежелательному принятию рисков. Бюджет, утвержденный на средства управления, следует использовать в качестве ограничивающего фактора только с крайней осторожностью.

В Приложении А приводятся примеры выбора конкретных средств управления из стандарта *СТ РК ИСО/МЭК 17799* в соответствии с количеством угроз, указанным в примере.

5.7.2 Уменьшение и принятие рисков

Для всех рисков, для которых в 5.6 выше был выбран вариант «уменьшение риска», следует выбрать необходимые средства управления, позволяющие уменьшить риски до уровня, который был определен в качестве приемлемого. Для идентификации средств управления полезно рассмотреть требования безопасности, связанные с этими рисками (т.е. угрозы и уязвимости, правовые и бизнес-требования), и все остальные результаты оценки рисков. Средства управления позволяют уменьшить оцененный риск несколькими различными способами, например:

уменьшая вероятность угрозы или вероятность уязвимости, которые приводят к данному риску;

обеспечивая выполнение правовых требований и бизнес-требований;

уменьшая возможное воздействие в случае возникновения риска;

обнаруживая нежелательные события, реагируя на них и выполняя восстановление.

Выбор организацией одного из перечисленных способов (или их комбинации) для обеспечения защиты своих ресурсов внутри данной СУИБ является бизнес-решением и зависит от условий бизнеса и обстоятельств, в которых приходится работать организации. Всегда важно соблюдать соответствие средств управления с конкретными потребностями организации и обосновывать принятое решение.

После идентификации подходящих средств управления, позволяющих уменьшить риск до приемлемого уровня, необходимо оценить, в какой именно степени эти средства управления, в случае их реализации, уменьшат риск – этот уменьшенный риск называется остаточным риском. Обычно этот остаточный риск оценить трудно, но, по крайней мере, следует сделать оценки того, насколько средства управления уменьшают уровень оценки соответствующих требований безопасности – это позволит гарантировать обеспечение защиты на достаточном уровне.

Если остаточный риск является неприемлемым, необходимо принять бизнес-решение о том, что с ним делать дальше. Один из возможных вариантов состоит в выборе дополнительных средств управления, чтобы в конечном счете уменьшить этот риск до приемлемого уровня. Хотя обычно рекомендуется не допускать оставления неприемлемых рисков, уменьшение всех рисков до приемлемого уровня не всегда может быть возможно или осуществимо с финансовой точки зрения.

После реализации выбранных средств управления риски остаются в любом случае. Информационные системы организации нельзя сделать

абсолютно безопасными. Вследствие этого, необходимо проверить реализацию и результаты действия средств управления (такие, как отчеты об инцидентах или файлы журналов), чтобы окончательно оценить, насколько хорошо работают реализованные средства управления. Эти действия являются частью этапа «Оценка» в модели ПРОК, и после этого идентифицированные усовершенствования должны быть реализованы на этапе «Корректировка» для более эффективного обеспечения безопасности.

Результат этапа 5.6:

В результате данного этапа должны быть выбраны средства управления, позволяющие уменьшить все риски, которые были идентифицированы на этапе 5.6 для обработки с помощью данного варианта. Кроме того, должны быть документированы связи с результатами оценки рисков, и должно быть обеспечено уменьшение всех рисков в максимально возможной степени.

6 Подходы к оценке рисков

6.1 Введение

В разделе 5 приводится описание процессов общей оценки рисков. Как уже говорилось в разделе 5, выбирать необходимый подход к оценке рисков должна сама организация, поэтому в данном разделе описываются различные варианты для подхода к оценке рисков. Эти различные подходы отличаются требуемым количеством времени и объемом работы, а также глубиной анализа деталей. Несмотря на то, что организация может сама выбирать подход к оценке рисков, необходимо гарантировать, что применяемый подход (подходы) оценки рисков является в достаточной мере адекватным и подробным, чтобы обеспечить выполнение бизнес-требований и требований безопасности организации.

Если, например, организация или СУИБ и ее ресурсы имеют бизнес-требования не выше низкого и среднего уровня, то может быть достаточно подхода Базисная оценка рисков (Basic Risk Assessment) (см. 6.2). Если требования безопасности имеют более высокий уровень, требующий более подробной и специальной оценки, то может потребоваться подход Детальная оценка рисков (Detailed Risk Assessment) (см. 6.3 и 6.4). В любом случае, необходимо гарантировать, что выбранный подход соответствует всем критериям, приведенным в стандарте *СТ РК ИСО/МЭК 27001*, а именно:

идентификация ресурсов (см. 5.1);

идентификация угроз и уязвимостей, а также всех других необходимых требований безопасности (см. 5.3);

идентификация воздействий, которые может оказать на ресурсы потеря конфиденциальности, целостности и доступности (см. 5.2);

на основе вышеперечисленной информации оценка ущерба и вероятности возникновения риска, а также оценка уровней рисков (см. 5.4 и 5.5);

идентификация наиболее подходящего варианта обработки рисков (см. 5.6);

выбор целей управления и средств управления для уменьшения рисков до приемлемого уровня (см. 5.7).

6.2 Базисная оценка рисков

Базисный подход предполагает выбор совокупности средств управления безопасностью на основе прямого и непосредственного применения процесса, описанного в разделе 5.

Этот подход позволяет организации разрабатывать свои СУИБ, достигая базисного уровня[4] защиты, на основе идентификации и оценки основных и важнейших потребностей и требований организации. Базисный уровень защиты, достигаемый с помощью этого непосредственного и простого в применении подхода, может подойти для какой-либо части организации с низким уровнем требований безопасности, или – в некоторых случаях – даже для всей организации, если ее требования безопасности имеют достаточно низкий уровень требований безопасности. Но для любой организации при сертификации по стандарту *СТ РК ИСО/МЭК 27001* важно суметь обосновать достаточность базисного подхода, если был выбран именно он.

Типичным примером применения данного подхода может являться часть организации, в которой проводятся не слишком сложные бизнес-операции и зависимость которой от обработки информации и работы в сети не очень велика. Этот подход возможен также в случае некоторых небольших организаций. Однако могут быть и небольшие организации, которые имеют более сложную бизнес-среду, зависят от широкого использования технологий, основанных на информационных системах, и принимают участие в обработке коммерчески важной информации.

В контексте стандарта *СТ РК ИСО/МЭК 27001* данный подход обязательно включает в себя систематическую оценку бизнес-требований организации (см. 5.3 и 5.4) для информации и рассматриваемых ресурсов, идентификацию подлежащих реализации целей управления и последующий выбор средств управления, удовлетворяющих этим целям.

Подход Базисная оценка рисков включает в себя следующие действия, основанные на процессах, описанных в разделе 5, и должен учитывать требования безопасности из всех источников.

---

[4] *Иногда называется базовым уровнем безопасности.*

Задачи оценки рисков и управления рисками	**Действия при выполнении Базисной оценки рисков**
Идентификация и оценка ресурсов (5.1 и 5.2)	Составить список ресурсов, связанных с данной бизнес-средой, операциями и информацией, оцениваемой в пределах области применения СУИБ, и определить уровень их важности, используя простую шкалу оценки.
Идентификация и оценка требований безопасности (5.3 и 5.4)	Идентифицировать требования безопасности (при этом можно использовать контрольные списки обобщенных или широко известных угроз и уязвимостей) и определить уровень всех идентифицированных требований безопасности, используя простую шкалу оценки.
Расчет рисков (5.5)	Рассчитать риски на основе информации о ресурсах и требованиях безопасности, используя простую схему расчета.
Идентификация и оценивание вариантов обработки рисков (5.6)	Идентифицировать подходящий вариант обработки риска для каждого из идентифицированных рисков; документировать результаты для плана обработки рисков.
Выбор средств управления безопасностью, уменьшение и принятие рисков (5.7)	Для каждого из идентифицированных ресурсов идентифицировать являющиеся значимыми цели управления и средства управления из стандарта *СТ РК ИСО/МЭК 17799-2005*. Гарантировать, что выбранные цели управления и средства управления уменьшают риски до приемлемого уровня.

Использование списков обобщенных или широко известных угроз и уязвимостей может помочь направить и ориентировать процесс анализа после действий по оценке. Более подробная информация об этом базисном подходе и соответствующем выборе средств управления приводится в [4].

Этот подход может применяться с помощью упрощенной версии табличного метода, описанного в Приложении Б (см. Б.2.2). При таком подходе могут использоваться, например, два уровня требований безопасности (например, Высокий и Низкий) и оценка ресурсов по ранее определенной шкале (например, Высокий уровень, Средний уровень и Низкий уровень).

Числа в приведенной ниже таблице показывают степень риска (например, от 0 до 4).

	Уровень требований безопасности	**Низкий**	**Высокий**
Оценка значимости ресурса	Низкий уровень	0	2
	Средний уровень	1	3
	Высокий уровень	2	4

Эти степени риска можно использовать, чтобы решить, какие риски необходимо обработать первыми и каким следует уделить больше внимания, а также определить, какие могут быть использованы варианты обработки рисков. Для тех рисков, для которых выбран вариант уменьшения риска, необходимо идентифицировать приемлемый уровень риска, соответствующий бизнес-требованиям и требованиям безопасности для рассматриваемой СУИБ. Для приведенного выше примера таблицы рекомендуется, чтобы приемлемый уровень риска не выбирался выше 2.

Подход Базисная оценка рисков имеет ряд преимуществ, таких как:

Для оценки рисков требуется минимум ресурсов, уменьшаются затраты времени и объем работы, необходимые для выбора средств управления. Обычно для идентификации необходимых средств управления не требуются значительные ресурсы,

Идентичные или похожие средства управления могут быть легко адаптированы для нескольких ресурсов. Если большинство ресурсов организации функционирует в общей среде, и если бизнес-требования и требования безопасности являются подобными, то эти средства управления могут обеспечить экономически эффективное решение.

Данный подход имеет следующие недостатки:

если уровень безопасности является очень высоким, то для некоторых ресурсов могут быть выбраны слишком дорогостоящие или излишне ограничительные средства управления, а если этот уровень является низким, реализованной безопасности может оказаться недостаточно для некоторых ресурсов;

могут возникнуть трудности в управлении значимыми для безопасности изменениями (как это требуется на этапах «Оценка» и «Корректировка» в модели ПРОК). Например, если происходят изменения во всей СУИБ, может быть затруднительно оценить, достаточно ли первоначальных средств управления в новой ситуации.

6.3 Детальная оценка рисков

Данный подход охватывает проведение детальной оценки рисков, включая детальную идентификацию и оценку ресурсов, а также идентификацию и оценку уровней требований безопасности. Эта информация используется для оценки рисков и последующей идентификации и выбора средств управления безопасностью.

Выбор средств управления обосновывается идентифицированными рисками, которым подвергаются ресурсы, и обеспечивается уменьшение этих рисков до приемлемого уровня (если был выбран данный вариант обработки риска).

Детальная оценка рисков может быть очень ресурсоемким процессом, и поэтому требуется тщательное определение границ бизнес-среды, операций,

информации и ресурсов в области применения оцениваемой СУИБ. Кроме того, подобный подход требует постоянного внимания со стороны руководства.

В соответствии с оцененными рисками, средства управления могут быть выбраны из стандарта *СТ РК ИСО/МЭК 17799* в связи с целями управления, которые должны быть достигнуты. Данный общий подход отличается от подхода Базисная оценка рисков, описанного в 6.2, тем, что выполняется более детальный анализ ресурсов и требований безопасности на принципах, описанных в разделе 5, и тем, что для соотнесения различных оценок и расчета рисков используется метод оценки, аналогичный одному из приведенных в Приложении Б.

Задачи оценки рисков и управления рисками	**Действия при выполнении Детальной оценки рисков**
Идентификация и оценка ресурсов (5.1 и 5.2)	Идентифицировать и составить список всех ресурсов, связанных с бизнес-средой, операциями и информацией в пределах области применения данной СУИБ, задать шкалу оценок и для каждого ресурса определить оценки по данной шкале (по одной оценке для каждого фактора: конфиденциальности, целостности и доступности, а также, при необходимости, любого другого фактора).
Идентификация требований безопасности (5.3)	Идентифицировать все требования безопасности (угрозы и уязвимости, правовые требования и бизнес-требования), связанные со списком ресурсов, находящихся в области применения СУИБ.
Оценка требований безопасности (5.4)	Идентифицировать необходимую шкалу оценок для требований безопасности и определить соответствующую оценку для каждого из идентифицированных требований безопасности.
Расчет рисков (5.5)	Рассчитать риски (исходя из ресурсов и требований безопасности, а также уровней их значимости, полученных в результате указанного выше оценивания) с помощью, например, одного из методов оценки рисков, приведенных в Приложении Б, или какой-либо их разновидности или аналогичного метода, соответствующего требованиям безопасности рассматриваемой СУИБ.
Идентификация и оценивание вариантов обработки рисков (5.6)	Идентифицировать подходящее действие по обработке риска для каждого из идентифицированных рисков. Оценить реалистичность идентифицированного варианта, его адекватность и соответствие всем бизнес-требованиям и требованиям безопасности. Документировать результаты для плана обработки рисков.
Выбор средств управления безопасностью,	Определить приемлемый уровень риска для выбранного метода оценки рисков и гарантировать соответствие этого уровня приемлемого риска бизнес-требованиям и требованиям

уменьшение и принятие рисков (5.7)	безопасности рассматриваемой СУИБ. Для тех рисков, для которых был выбран вариант уменьшения риска, выбрать из стандарта *СТ РК ИСО/МЭК 17799* подходящие цели управления и средства управления, позволяющие уменьшить эти риски до приемлемого уровня. Оценить, в какой степени выбранные средства управления уменьшают идентифицированные риски. Для каждого риска, который не может быть уменьшен до приемлемого уровня, идентифицировать дополнительные действия по его обработке (либо утверждение руководством принятия этого риска по соображениям бизнеса, либо дальнейшее уменьшение риска).

Преимущества этого подхода заключаются в следующем:

достигается точное и детальное представление о рисках безопасности, которое позволяет получить идентификацию уровней безопасности, отражающую требования безопасности организации к ресурсам и СУИБ;

при управлении значимыми для безопасности изменениями (как это требуется на этапах «Оценка» и «Корректировка» модели ПРОК) можно использовать дополнительную информацию, полученную в результате детальной оценки рисков.

Этот подход имеет следующий недостаток:

для получения качественных результатов требуется значительное количество времени, большой объем работы и высокая квалификация.

6.4 Комбинированный подход

Этот подход предполагает идентификацию в первую очередь тех ресурсов из области применения СУИБ, которые потенциально имеют высокий уровень риска или являются критичными для бизнес-операций.

На основании этих результатов все ресурсы, входящие в область применения СУИБ, подразделяются на ресурсы, для достижения надлежащей защиты которых требуется проведение Детальной оценки рисков (см. 6.3), и ресурсы, для которых достаточно подхода Базисная оценка рисков (см. 6.2). Такой подход позволяет объединить преимущества подходов, описанные выше в 6.2 и 6.3. Вследствие этого, он является хорошим компромиссом, позволяющим минимизировать время и усилия, которые тратятся на идентификацию средств управления, и обеспечивающим при этом надлежащую оценку и защиту ресурсов организации.

Помимо объединения преимуществ двух подходов, данный подход имеет также и то преимущество, что:

средства и деньги могут быть применены там, где от них будет наибольшая польза, а информационные системы организации, которые,

вероятнее всего, имеют высокий уровень риска, могут быть учтены в первую очередь.

Данный подход имеет следующий недостаток:

подход может привести к ошибочным результатам в случае неправильной идентификации информационных систем, имеющих высокий уровень риска, т.е. если к системам, для которых требуется Детальная оценка рисков, будет применен только подход Базисная оценка рисков.

6.5 Выбор необходимого подхода к оценке рисков/управлению рисками

6.5.1 Факторы, влияющие на выбор

Для оценки рисков организация может выбирать различные общие, используемые во всей организации, подходы. В предыдущих пунктах этого раздела были указаны некоторые преимущества и недостатки таких подходов. Какой именно подход использовать организации, зависит от нескольких факторов, в том числе от:

- их бизнес-среды и вида бизнес-деятельности;
- зависимости от обработки информации и приложений, поддерживающих бизнес;
- сложности бизнес-систем и поддерживающих систем, приложений и сервисов;
- количества компаний-партнеров и объема внешних деловых и договорных отношений.

Эти факторы должны быть, как правило, общими для всех направлений деятельности, поэтому при выборе нужного подхода для всей организации необходимо учитывать эти факторы наряду с преимуществами и недостатками самих подходов. Принимать решение о выборе подхода должна сама организация при условии соблюдения критериев, установленных в стандарте *СТ РК ИСО/МЭК 27001* (см. 6.1). На практике рекомендуется придерживаться следующего правила: чем более важной и необходимой является безопасность для организации и ее бизнеса, и чем больше могут быть потери, тем больше времени и средств необходимо потратить на обеспечение безопасности.

6.5.2 Сертификация СУИБ по стандарту *СТ РК ИСО/МЭК 27001*

Для сертификации систем управления информационной безопасностью (СУИБ) по стандарту *СТ РК ИСО/МЭК 27001* необходимо выполнение требования о проведении надлежащей оценки рисков и документировании результатов этой оценки в Положении о применимости. Это условие является важной частью процесса сертификации, и поэтому в той же мере важно, чтобы организация выбрала наиболее адекватный подход к оценке рисков.

6.6 Оценка рисков и малые и средние предприятия

Не существует общего правила, которое определяло бы, какой подход к оценке рисков лучше использовать для малых и средних предприятий, поскольку это решение должно основываться на бизнес-требованиях и требованиях безопасности, и необязательно зависит от размера организации. Ниже приводится несколько замечаний для малых и средних предприятий, основанных на некоторых общих представлениях о том, каким образом они могут соотносить факторы, перечисленные в 6.5.1.

Безусловный факт, что, чем менее сложными являются бизнес-операции и чем меньше имеется систем, тем более простыми могут быть требования к информационной безопасности, и эта ситуация, вероятно, остается верной для большей части малых и средних предприятий.

Однако существуют малые и средние предприятия, бизнес-требования которых могут быть очень сложными. Предприятие малого и среднего бизнеса может быть поставщиком для многих организаций, и может быть заключен договор о реализации ряда средств управления из стандарта *СТ РК ИСО/МЭК 17799*. Например, такому предприятию необходимо учесть аспекты из раздела «Безопасность доступа сторонних организаций» стандарта *СТ РК ИСО/МЭК 17799*, а также рассмотреть вопрос, следует ли применять какие-либо аспекты из раздела «Соглашения об обмене данными и программами», разделов «Управление доступом к сети/компьютерам/приложениям» и «Разработка и сопровождение информационных систем» в связи с их ролью поставщика различных услуг и продуктов. Кроме того, им, несомненно, потребуется определить, какие аспекты раздела «Соответствие формальным требованиям» следует применить.

Зависимость предприятия от обработки информации и использования вычислительных систем может быть очень высокой, и их бизнес может в значительной мере определяться использованием подобных систем. Например, малое и среднее предприятие может использовать эти системы для производства информационных продуктов для индустрии развлечений, где содержание и дизайн имеют высокую рыночную стоимость в терминах интеллектуальной собственности.

Средним и малым предприятиям необходимо найти баланс между средствами, которые потребуется затратить на оценку рисков в соответствии с одним из трех подходов (см. 6.2, 6.3 и 6.4), и реализацией средств управления безопасностью, которые удовлетворяли бы собственным требованиям безопасности и требованиям заказчиков. Как минимум, средним и малым предприятиям, каким бы ни был их бизнес, потребуется реализовать некоторые средства управления безопасностью, и подход Базисная оценка рисков позволит им определить, какие это должны быть

средства управления. Безусловно, существует необходимость реализовать политику безопасности в той или иной форме, установить несколько средств контроля доступа и соблюдать правовые и нормативные требования. Кроме того, может потребоваться специально рассмотреть некоторые конкретные требования, возникающие в результате деловых отношений, с помощью подхода Детальная оценка рисков, как это описано в разделе 6.3.

Приложение А
(справочное)
Примеры угроз и уязвимостей

Нижеприведенные списки содержат несколько примеров угроз и уязвимостей, связанных с целями управления и средствами управления, указанными в стандарте *СТ РК ИСО/МЭК 17799*. Эти списки угроз и уязвимостей не являются исчерпывающими, и их следует рассматривать только в качестве примеров, иллюстрирующих эти понятия и связь со средствами управления, приведенными в стандарте *СТ РК ИСО/МЭК 17799*.

И в этом случае наиболее важный принцип заключается в том, что организации нужно принять подходы к оценке рисков и управлению рисками, которые должным образом учитывали бы и идентифицировали полный диапазон угроз и уязвимостей, значимых для их бизнес-среды. Этот диапазон может включать все угрозы и уязвимости, перечисленные в приведенных ниже списках, или их часть.

А.1 Пример списка угроз

Ниже приводится примерный список угроз, полученный из [3]. Этот список угроз приводится здесь для иллюстрации и не должен рассматриваться как полный и окончательный.

Частицы аэрозоля/пыли	Аппаратный сбой
Неисправность в системе кондиционирования	Ураган
Террористический акт	Незаконный импорт/экспорт программного обеспечения
Несанкционированное проникновение в системы связи	Незаконное использование программного обеспечения
Повреждение линий/кабелей связи	Забастовка
Разрушение носителей информации	Попадание молнии
Землетрясение	Ошибка технического обслуживания
Подслушивание	Вредоносное программное обеспечение (например, вирусы, сетевые черви, троянские кони)
Загрязнение окружающей среды (и другие формы природных или антропогенных катастроф)	Подмена идентификационной информации пользователя
Экстремальные значения температуры и важности	Неправильная маршрутизация или перемаршрутизация сообщений
Отказ сервисов связи	Сетевой доступ неавторизованных пользователей
Сбой компонентов сети	Неправильное использование ресурсов
Отказ в системе питания	Ошибка персонала оперативной поддержки
Авария водопровода	Броски по питанию
Пожар	Возможность отказа (например, от услуг, транзакций, получения/отправления сообщений

Наводнение	Сбой в программном обеспечении
Нехватка персонала	Несанкционированное использование носителей данных
Кража	Использование средств связи несанкционированным образом
Анализ трафика	Использование программного обеспечения неавторизованными пользователями
Перегрузка трафика	Использование программного обеспечения несанкционированным образом
Ошибка передачи данных	Ошибка пользователя
Несанкционированное использование программного обеспечения	Намеренное причинение ущерба

В зависимости от типа угрозы, ее осуществление может привести к различным последствиям, таким как:

Случайные или непреднамеренные изменения в средствах, обеспечивающих совместное использование данных и программного обеспечения в вычислительной среде.	Нарушение безопасности в результате несоблюдения технических инструкций.
Нарушение безопасности вследствие неточных, неполных или несоответствующих технических или должностных инструкций, или недостаточного обновления этих процедур.	
Нарушение безопасности в результате несоблюдения процедур обработки инцидентов.	Компрометация, потеря данных на площадке подрядчика.
Ущерб вследствие неточных, неполных или несоответствующих планов обеспечения бесперебойной работы, недостаточного тестирования или недостаточного обновления этих планов	
Отказ в обслуживании, в предоставлении системных ресурсов, в предоставлении информации	Почтовые бомбы (E-mail bombs)
Подлог	Мошенничество
Небрежное или преднамеренное неправильное использование средств вследствие отсутствия разделения и выполнения обязанностей	Несанкционированное раскрытие местонахождения площадок/зданий/помещений, содержащих критичные и/или важные вычислительные средства и средства обработки
Несанкционированное раскрытие информации	

А.2 Примеры угроз и стандарты *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001*

Ниже приводится пример того, как различные угрозы, перечисленные выше, связаны с приведенными в стандартах *СТ РК ИСО/МЭК 17799* и *СТ РК ИСО/МЭК 27001* целями управления.

А.2.1 Физическая безопасность и безопасность среды функционирования

Защищенные области

Цель: Предотвратить несанкционированный физический доступ к производственным помещениям и информационным сервисам, их повреждение и вмешательство в их функционирование.

ИТ-средства, поддерживающие критичные или важные бизнес-операции, должны быть размещены в защищенных областях.

Пожар	Наводнение
Террористический акт	Ураган
Землетрясение	Забастовка
Загрязнение окружающей среды (и другие формы природных или антропогенных катастроф)	Попадание молнии
Кража	Намеренное причинение ущерба

Защита оборудования

Цель: Предотвратить потерю, повреждение или компрометацию ресурсов, а также перебои в работе организации.

Необходимо обеспечить физическую защиту оборудования от угроз нарушения безопасности и опасностей, представляемых окружающей средой.

Частицы аэрозоля/пыли	Аппаратный сбой
Неисправность в системе кондиционирования	Ошибка технического обслуживания
Террористический акт	Вредоносное программное обеспечение (например, вирусы, сетевые черви, троянские кони)
Загрязнение окружающей среды (и другие формы природных или антропогенных катастроф)	Сетевой доступ неавторизованных пользователей
Отказ в системе питания	Броски по питанию
Пожар	Кража
Наводнение	Ошибка пользователя
Намеренное причинение ущерба	

А.2.2 Администрирование компьютерных систем и вычислительных сетей

Операционные процедуры и обязанности

Цель: Обеспечить корректное и надежное функционирование средств, используемых для обработки информации.

Необходимо определить обязанности и процедуры по администрированию и обеспечению функционирования всех компьютеров и сетей.

Неисправность в системе кондиционирования	Подмена идентификационной информации пользователя
Террористический акт	Неправильная маршрутизация или перемаршрутизация сообщений
Несанкционированное проникновение в системы связи	Неправильное использование ресурсов
Землетрясение	Сетевой доступ неавторизованных пользователей
Отказ в системе питания	Ошибка персонала оперативной поддержки
Пожар	Сбой в программном обеспечении
Наводнение	Кража
Аппаратный сбой	Перегрузка трафика
Ураган	Ошибка передачи данных
Забастовка	Использование программного обеспечения неавторизованными пользователями
Попадание молнии	Использование программного обеспечения несанкционированным образом
Ошибка технического обслуживания	Ошибка пользователя
Вредоносное программное обеспечение (например, вирусы, сетевые черви, троянские кони)	Намеренное причинение ущерба

А.2.3 Планирование бесперебойной работы организации

Аспекты планирования бесперебойной работы организации

Цель: Противодействовать перебоям в работе организации и обеспечить защиту критических производственных процессов от последствий крупных аварий и катастроф.

Террористический акт	Ураган
Несанкционированное проникновение в системы связи	Забастовка
Загрязнение окружающей среды (и другие формы природных или антропогенных катастроф)	Попадание молнии
Отказ сервисов связи	Нехватка персонала
Пожар	Наводнение
Намеренное причинение ущерба	

А.2.4 Соответствие формальным требованиям

Выполнение правовых требований

Цель: Избежать нарушения уголовного и гражданского законодательства, имеющих силу закона обязательств, регулирующих или договорных обязательств, а также требований к информационной безопасности.

На разработку, сопровождение и использование информационных систем могут быть наложены правовые и договорные требования к безопасности.

Террористический акт	Неправильное использование ресурсов
Несанкционированное проникновение в системы связи	Сетевой доступ неавторизованных пользователей
Подслушивание	Кража
Незаконный импорт/экспорт программного обеспечения	Несанкционированное использование программного обеспечения
Незаконное использование программного обеспечения	Использование средств связи несанкционированным образом
Подмена идентификационной информации пользователя	Использование программного обеспечения несанкционированным образом

Проверка безопасности информационных систем

Цель: Обеспечить соответствие систем принятым в организации политикам и стандартам безопасности.

Безопасность информационных систем необходимо регулярно проверять.

Террористический акт	Неправильное использование ресурсов
Несанкционированное проникновение в системы связи	Сетевой доступ неавторизованных пользователей
Подслушивание	Кража
Отказ сервисов связи	Несанкционированное использование программного обеспечения
Незаконный импорт/экспорт программного обеспечения	Использование средств связи несанкционированным образом
Незаконное использование программного обеспечения	Использование программного обеспечения неавторизованными пользователями
Вредоносное программное обеспечение (например, вирусы, сетевые черви, троянские кони)	Использование программного обеспечения несанкционированным образом
Подмена идентификационной информации пользователя	Намеренное причинение ущерба

Аудит систем

Цель: Минимизировать воздействие, с одной стороны, процесса аудита на информационные системы, а с другой – информационных систем на процесс аудита.

Необходимо иметь средства контроля для защиты рабочих систем и средств аудита во время их проверки.

Несанкционированное проникновение в системы связи	Подмена идентификационной информации пользователя
Подслушивание	Неправильное использование ресурсов
Отказ сервисов связи	Сетевой доступ неавторизованных пользователей
Незаконный импорт/экспорт программного обеспечения	Кража
Незаконное использование программного обеспечения	Несанкционированное использование программного обеспечения
Вредоносное программное обеспечение (например, вирусы, «сетевые черви», «троянские кони»)	Использование сетевого оборудования несанкционированным образом

А.3 Пример списка уязвимостей

В приведенных ниже списках содержатся примеры уязвимостей в различных областях безопасности, а также примеры угроз, которые могут использовать эти уязвимости. Эти списки могут быть полезны при проведении оценки уязвимостей.

Следует особо отметить, что другие угрозы также могут использовать эти уязвимости.

А.3.1 Аспекты безопасности, связанные с персоналом (*СТ РК ИСО/МЭК17799*)

Уязвимость	Уязвимость используется угрозой
Отсутствие персонала	Нехватка персонала
Отсутствие контроля за внештатными сотрудниками или за сотрудниками, убирающими помещения	Кража
Недостаточное обучение безопасности	Ошибка персонала оперативной поддержки
Недостаточная информированность по вопросам безопасности	Ошибки пользователей
Плохо документированное программное обеспечение	Ошибка персонала оперативной поддержки
Отсутствие механизмов контроля	Использование программного обеспечения несанкционированным образом
Отсутствие политик корректного использования средств телекоммуникации и обмена сообщениями	Использование средств связи несанкционированным образом
Невыполнение процедур приема на работу	Намеренное причинение ущерба

А.3.2 Физическая безопасность и безопасность среды функционирования (ИСО/МЭК 17799)

Уязвимость	Уязвимость используется угрозой
Отсутствие или небрежное осуществление контроля физического доступа в здания, помещения и комнаты	Намеренное причинение ущерба
Отсутствие физической защиты здания, дверей и окон	Кража
Расположение в области, в которой возможны наводнения	Наводнение
Незащищенное хранение	Кража
Недостаточное сопровождение/неправильная установка носителей информации	Ошибка технического обслуживания
Отсутствие планов периодической замены оборудования	Разрушение носителей информации
Чувствительность оборудования к влажности, пыли, загрязнению	Частицы аэрозоля/пыли
Чувствительность оборудования к колебаниям температуры	Экстремальные значения температуры
Чувствительность оборудования к колебаниям напряжения	Броски по питанию
Нестабильная работа системы электропитания	Броски по питанию

А.3.3 Администрирование компьютерных систем и вычислительных сетей (ИСО/МЭК 17799)

Уязвимость	Уязвимость используется угрозой
Незащищенные линии связи	Подслушивание
Неудовлетворительное состояние кабельных соединений	Несанкционированное проникновение в системы связи
Отсутствие механизмов идентификации и аутентификации	Подмена идентификационной информации пользователя
Передача паролей в явном виде	Сетевой доступ неавторизованных пользователей
Отсутствие подтверждения отправки или получения сообщений	Отказ от своих действий
Коммутируемые линии	Сетевой доступ неавторизованных пользователей
Незащищенность трафика важной информации	Подслушивание
Единственная точка отказа	Отказ сервисов связи
Не отвечающее требованиям сетевое управление	Перегрузка трафика
Отсутствие контроля за утилизацией	Кража

Неконтролируемое копирование	Кража
Незащищенные подключения к общедоступной сети	Использование программного обеспечения неавторизованными пользователями

А.3.4 Управление доступом/Разработка и сопровождение информационных систем (ИСО/МЭК 17799)

Уязвимость	Уязвимость используется угрозой
Сложный интерфейс пользователя	Ошибка персонала оперативной поддержки
Утилизация или повторное использование носителей информации без надлежащего удаления информации	Использование программного обеспечения неавторизованными пользователями
Отсутствие контрольных журналов	Использование программного обеспечения несанкционированным образом
Отсутствие документации	Ошибка персонала оперативной поддержки
Отсутствие эффективного контроля за изменениями	Сбой в программном обеспечении
Отсутствие механизмов идентификации и аутентификации	Подмена идентификационной информации пользователя
Неиспользование процедуры выхода из системы после прекращения работы на компьютере	Использование программного обеспечения неавторизованными пользователями
Отсутствие или недостаточность тестирования программного обеспечения	Использование программного обеспечения неавторизованными пользователями
Неудовлетворительное управление паролями (легко отгадываемые пароли, хранение паролей, недостаточно регулярная смена паролей)	Подмена идентификационной информации пользователя
Нечеткие или неполные спецификации для разработчиков	Сбой в программном обеспечении
Неконтролируемая загрузка и использование программного обеспечения	Вредоносное программное обеспечение
Незащищенные таблицы паролей	Подмена идентификационной информации пользователя
Известные бреши в программном обеспечении	Использование программного обеспечения неавторизованными пользователями
Ошибочное распределение прав доступа	Использование программного обеспечения несанкционированным образом

Приложение Б
(справочное)
Инструментальные средства и методы

Б.1 Инструментальные средства

Для проведения оценки рисков и управления рисками разработаны разнообразные методы, начиная от простых подходов, основанных на анкетах с вопросами и ответами, и заканчивая методами, использующими структурный анализ. В продаже имеется множество инструментальных средств, предназначенных для содействия процессу оценки. К ним относятся как автоматизированные (компьютерные), так и неавтоматизированные продукты.

Б.1.1 Критерии для выбора средства оценки рисков

Какие бы методы и продукты ни использовались организацией, они должны, по меньшей мере, учитывать компоненты, связи между компонентами и процессы, описанные в разделах 5 и 6 настоящего стандарта.

Завершив в первый раз процесс оценки рисков, необходимо сохранить и документировать результаты этого процесса (ресурсы и оценки их значимости, требования безопасности и уровни рисков, а также идентифицированные средства управления), например, в базе данных. Средства программной поддержки могут значительно облегчить эту работу, а также все будущие действия по повторной переоценке.

Что должно обеспечивать средство для оценки рисков? Приводимый ниже список позволяет получить некоторое представление о критериях, которые следует учесть при выборе средства для оценки рисков:

Это средство должно, по меньшей мере, содержать следующие модули:

сбора данных,

анализа,

вывода результатов.

Метод, на основе которого работает и функционирует выбранное средство, должен отражать политику организации и общий подход к оценке рисков.

Если в процессе управления требуется выполнить сравнение альтернативных вариантов и выбрать адекватные, надежные и экономически эффективные средства управления, то важнейшей частью этого процесса является эффективное предоставление результатов, поэтому данное средство должно обеспечивать предоставление результатов в понятном и четком виде.

Возможность вести архив информации, полученной на этапе сбора данных, и архив аналитических данных может пригодиться при проведении последующих оценок рисков или запросов.

Должна быть доступна документация, описывающая данное средство, поскольку она играет важную роль в его эффективном использовании.

Выбранное средство должно быть совместимо с программным и аппаратным обеспечением, используемым в организации.

Автоматизированные средства, как правило, эффективны и свободны от ошибок, но некоторые из них могут иметь сложные процессы установки или использования, поэтому может возникнуть необходимость рассмотреть доступность программ обучения и поддержки.

Эффективное применение данного средства частично зависит от того, насколько хорошо пользователь понимает этот продукт, а также от корректной установки и конфигурации используемого средства, поэтому большое значение может иметь наличие руководства по установке и использованию.

Б.2 Типы и примеры методов оценки рисков

Б.2.1 Обзор процесса оценки рисков

Процесс оценки рисков состоит из нескольких этапов, которые были описаны в Разделе 3:

Идентификация и оценивание ресурсов (см. 5.1 и 5.2);

Идентификация и оценивание требований безопасности (т.е. угроз и уязвимостей, правовых требований и бизнес-требований, см. также 5.3 и 5.4);

Расчет рисков (см. 5.5);

Идентификация подходящего варианта обработки рисков (см. 5.6);

Выбор средства управления для уменьшения рисков до приемлемого уровня (см. 5.7).

Цель оценки рисков состоит в идентификации и оценке рисков, которым подвергаются информационная система и ее ресурсы, для последующей идентификации и выбора подходящих и обоснованных средств управления безопасностью. Эта оценка, таким образом, основывается на стоимости ресурсов и на уровнях требований безопасности и учитывает существующие/запланированные средства управления. В данном Приложении рассматривается первая часть процесс оценки рисков, во время которой проводится идентификация и расчет рисков (Этапы 5.1–5.5 в разделе 5).

Значения стоимости ресурсов, или потенциальные воздействия на бизнес в случае возникновения инцидента, можно оценить несколькими способами, включая использование количественных (например, денежных) и качественных (которые могут основываться на таких характеристиках, как «средний» или «высокий») показателей, а также их комбинации. Трудоемкой частью процесса оценки рисков может быть оценка угроз и уязвимостей. Вероятность осуществления угрозы зависит от следующих факторов:

привлекательность ресурса – применяется, если рассматривается преднамеренная угроза со стороны человека;

легкость получения вознаграждения за ресурс – применяется, если рассматривается преднамеренная угроза со стороны человека;

технические возможности, необходимые для реализации угрозы – применяется, если рассматривается преднамеренная угроза со стороны человека;

вероятность угрозы;

восприимчивость уязвимости к использованию, применяется как к техническим, так и нетехническим уязвимостям.

Во многих методах оценки рисков применяются таблицы и совместно используются качественные и количественные показатели. Как уже говорилось ранее, не существует правильных и неправильных методов оценки рисков. Кроме того, что метод должен обеспечивать соблюдение требований, приведенных в стандарте *СТ РК ИСО/МЭК 27001*, также важно, чтобы организация использовала метод, который удобен самой организации, которому организация доверяет, и который позволит получать повторяемые результаты. Ниже приводятся несколько примеров методов, основанных на таблицах.

Б.2.2 Таблица для раздельной оценки угроз/уязвимостей

В данном примере угрозы и уязвимости не рассматриваются совместно в качестве причин инцидентов (как в 5.3), а учитываются отдельно. Это еще один возможный способ оценки рисков, который подробно описывается, например в [3], а также поддерживается несколькими инструментальными средствами. Если выбирается этот метод, то следует тщательно рассмотреть правовые и бизнес-требования.

Оценки ресурсов получаются по результатам интервьюирования выбранных сотрудников из бизнес-персонала («владельцев ресурсов»), которые могут авторитетно привести информацию, позволяющую определить стоимость и важность ресурса. Эти интервью способствуют выполнению оценки стоимости и важности ресурсов, исходя из наиболее неблагоприятных вариантов, которые могут, при разумных предположениях, реализоваться в результате таких инцидентов, как несанкционированное раскрытие, несанкционированная модификация, отказ от своих действий, недоступность в течение различных периодов времени и уничтожение.

Чтобы в этом методе учесть правовые и бизнес-требования, оценка ресурсов должна включать такие проблемы, как:

личная безопасность;
персональная информация;
правовые и нормативные обязательства;
правоприменение;
коммерческие и экономические интересы;
финансовые потери/прекращение работы;
общественный порядок;
бизнес-политика и бизнес-операции;
нематериальные потери.

На основе этой оценки необходимо для каждого возможного ущерба и для каждого ресурса определить соответствующий уровень на шкале оценок, в данном примере используется шкала от 1 до 4.

Следующим важным этапом является заполнение опросных листов для каждого ресурса и для всех угроз и уязвимостей, связанных с данным ресурсом, с целью обеспечить выполнение оценки для уровней угроз (вероятность осуществления) и уровней уязвимостей (легкости использования угрозами, в результате которого происходи инцидент). Каждый ответ на вопрос добавляет некоторый балл. Это позволяет идентифицировать уровни угроз и уязвимостей на заранее заданной шкале (в приведенном ниже примере используется шкала Низкий – Средний – Высокий, как это показано в таблице ниже). Для получения информации, используемой при заполнении опросных листов, необходимо провести интервьюирование сотрудников технического отдела, отдела кадров и хозяйственный отдел; проинспектировать возможное физическое местонахождение и проанализировать имеющуюся документацию.

Оценки стоимости ресурсов сопоставляются с уровнями угроз и уязвимостей с помощью таблицы, аналогичной той, которая приведена ниже. Для каждой комбинации идентифицируется подходящая степень риска на шкале от 1 до 8:

	Уровни угрозы	Низкий			Средний			Высокий		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Оценка ресурса	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для каждого ресурса рассматриваются уязвимости, относящиеся к этому ресурсу, и соответствующие им угрозы. Если имеется уязвимость без соответствующей угрозы, или угроза без соответствующей уязвимости, то риск отсутствует (но следует проявить осторожность, если ситуация изменится!). Теперь соответствующая строка в таблице идентифицируется оценкой ресурса, а соответствующий столбец – серьезностью угрозы и уязвимости. Например, если ресурс имеет оценку 3, уровень угрозы – «высокий», а уровень уязвимости – «низкий», то степень риска имеет значение 5.

В таблице может меняться количество уровней угроз, уровней уязвимостей и количество категорий оценки ресурсов, и, следовательно, эту таблицу можно корректировать в соответствии с потребностями организации. Использование дополнительных столбцов и строк влечет за собой дополнительные степени риска. Завершив в первый раз процесс оценки рисков, необходимо сохранить и документировать результаты этого процесса (ресурсы и оценки их значимости, требования безопасности и уровни рисков, а также идентифицированные средства управления), например, в базе данных. Средства программной поддержки могут значительно облегчить эту работу, а также все будущие действия по повторной переоценке.

Б.2.3 Ранжирование инцидентов по степени риска

Для сопоставления факторов воздействия (оценки ресурса) и вероятности инцидента (с учетом угроз и уязвимостей или любых других требований безопасности, которые могут вызвать конкретный инцидент) можно использовать таблицу. Первый шаг состоит в оценивании воздействия (оценки ресурса) для каждого ресурса по предварительно установленной шкале, например, от 1 до 5 (столбец «б» в приведенной ниже таблице). На втором шаге для каждого инцидента следует оценить вероятность инцидента по предварительно установленной шкале, например, от 1 до 5 (столбец «в» в приведенной ниже таблице). Третий шаг состоит в расчете степени риска с помощью умножения (б х в). Наконец, инцидентам может быть присвоена категория, соответствующая их коэффициенту «воздействия». Следует отметить, что в данном примере 1 обозначает наименьшее воздействие и наименьшую вероятность инцидента.

Идентификатор инцидента (а)	Оценка воздействия (ресурса) (б)	Вероятность возникновения инцидента (в)	Степень риска (г)	Ранг инцидента (д)
Инцидент А	5	2	10	2
Инцидент Б	2	4	8	3
Инцидент В	3	5	15	1
Инцидент Г	1	3	3	5
Инцидент Д	4	1	4	4
Инцидент Е	2	4	8	3

Как показано выше, такая процедура позволяет сравнивать различные инциденты, имеющие различное воздействие и различную вероятность, и она же, как показано здесь, позволяет ранжировать их в зависимости от приоритета. В некоторых случаях необходимо с используемыми здесь эмпирическими шкалами связать денежные значения.

Б.2.4 Оценка рисков для систем

В этом примере акцент делается на определении систем, которым следует отдавать приоритет с учетом инцидентов и их воздействий. Для этого определяются две оценки для каждого ресурса и риска, которые вместе позволяют определить балл для каждого ресурса. Степень риска для информационной системы вычисляется как сумма баллов по всем ресурсам.

Сначала каждому ресурсу присваивается некоторая оценка. Эта оценка обозначает потенциальный ущерб, который может возникнуть в случае, если реализации угрозы для данного ресурса. Эта оценка ресурса присваивается ресурсу для каждой угрозы, которой подвергается ресурс.

После этого для каждого инцидента оценивается вероятность инцидента, как это описано в Б.2.3. Затем, с помощью поиска пересечения оценки ресурса и значения вероятности инцидента в приведенной ниже таблице определяется балл для ресурса/инцидента.

Оценка ресурса	0	1	2	3	4
Вероятность инцидента					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

На заключительном шаге суммируются итоговые баллы для всех ресурсов данной системы, в результате чего получается оценка системы. Такую процедуру можно использовать, чтобы произвести дифференциацию систем и определить систему, защита которой должна быть получить приоритетное значение. Ниже приводится пример:

Допустим, Система S состоит из трех ресурсов Al, А2 и А3. Кроме того, допустим, что существуют два инцидента I1 and I2, которые могут возникнуть в системе S. Пусть оценка для Al равна 3, для А2 – 2, а для А3 – 4.

Если для ресурса А1 вероятность инцидента I1 равна l, то балл для ресурса/инцидента А1/I1 может быть получен из приведенной выше таблицы как пересечение оценки ресурса, равной 3, и вероятности инцидента, равной 1, т.е. этот балл будет равен 4. Подобным образом, если для ресурса А1 вероятность инцидента I2 равна 3, то балл для А1/I2 будет равен 6.

После этого можно рассчитать итоговый балл для ресурса А1 (Al_total) по всем инцидентам, а затем – рассчитать подобный итоговый балл для всех ресурсов и относящихся к ним угроз. Итоговый балл для системы рассчитывается с помощью сложения A1_total + A2_total + A3_total.

Таким образом можно выполнить сравнение систем и определить их приоритетность.

Б.2.5 Разграничение приемлемых и неприемлемых рисков

Еще один способ определения степени риска состоит только в разграничении приемлемых и неприемлемых рисков. Суть этого метода состоит в том, что степени риска используются только для определения тех рисков, для которых требуется наиболее срочное принятие мер.

При подобном подходе используемая таблица просто не будет содержать цифр, а будет состоять только из значений П и Н, показывающих, является риск приемлемым или неприемлемым. Например, таблица в Б.2.4 изменится следующим образом:

Оценка ущерба	0	1	2	3	4
Вероятность инцидента					
0	П	П	П	П	Н
1	П	П	П	Н	Н
2	П	П	Н	Н	Н
3	П	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

И в этом случае данная таблица является только примером, и пользователь сам может провести разграничивающую линию между приемлемыми и неприемлемыми рисками.

Приложение
(справочное)
Библиография

[1] BS ISO/IEC TR 13335-1:1996 Guidelines for the Management of IT Security (GMITS) Part 1: Concepts and Models for IT Security – [BS ISO/IEC TR 13335-1:1996 Руководства по управлению ИТ-безопасностью (GMITS), Часть 1: Концепции и модели для ИТ-безопасности]

[2] BS ISO/IEC TR 13335-2:1997 Guidelines for the Management of IT Security (GMITS) Part 2: Managing and Planning IT Security – [BS ISO/IEC TR 13335-2:1997 Руководства по управлению ИТ-безопасностью (GMITS), Часть 2: Управление и планирование ИТ-безопасности]

[3] BS ISO/IEC TR 13335-3:1998 Guidelines for the Management of IT Security (GMITS) Part 3: Techniques for the Management of IT Security – [BS ISO/IEC TR 13335-3:1998 Руководства по управлению ИТ-безопасностью (GMITS), Часть 3: Методы управления для ИТ-безопасности]

[4] BS ISO/IEC TR 13335-4:2000 Guidelines for the Management of ГГ Security (GMITS) Part 4: Selection of Safeguards – [BS ISO/IEC TR 13335-4:2000 Руководства по управлению ИТ-безопасностью (GMITS), Часть 4: Выбор мер безопасности]

[5] BS ISO/IEC PDTR 13335-5:2001 Guidelines for the Management of IT Security (GMITS) Part 5: Safeguards for External Connections [BS ISO/IEC PDTR 13335-5:2000 Руководства по управлению ИТ-безопасностью (GMITS), Часть 5: Меры безопасности для внешних соединений]

[6] БИС РД 3002:2002 «Руководство по оценке и управлению рисками по стандарту BS 7799» («Guide to BS 7799 risk assessment»)

[7] Protecting Business Information "Understanding the risks", published by the DTI, URN 96/939, 1996

[8] Protecting Business Information "Keeping it Confidential", published by the DTI, URN 96/938, 1996

[9] Information Security Assurance Guidelines for the commercial sector, published by the DTI, URN 99/697, 1999

[10] ISO Guide 73:2002 Risk Management – Vocabulary – Guidelines for use in standards (Управление рисками – Терминология – Руководство по использованию в стандартах)

[11] OECD Guide on security for information systems and networks, September 2002

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: сертификация, требования стандарта, система управления информационной безопасностью (СУИБ), оценка рисков, средства управления.

Для заметок

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074

Замечания и предложения к Указателю нормативных документов по стандартизации Республики Казахстан на 2009 год

№	Написано		Должно быть
	МКС	Наименование стандарта	МКС
1	35.060	СТ РК 34.029-2008 Информационная технология. Оценки управление рисками	35.240.01 03.120.01

(САС № 6-2009 ж.)
(ИУС № 6-2009 г.)